

Acer

WLAN 11g Broadband Router

User Manual



This product is in compliance with the essential requirements and other relevant provisions of the R&TTE directive 1999/5/EC.



Product Name: Acer WLAN 11g Broadband Router

Model Name : WLAN-G-RU2

COUNTRY		CHANNELS	MAX. OUT POWER	
			INDOOR	OUTDOOR
Spain	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
France	2400-2454 MHz	1-8	< 100 mW EIRP	< 100 mW EIRP
France	2454-2483.5 MHz	9-13	< 100 mW EIRP	< 10 mW EIRP
Italy	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
UK	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Netherlands	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Germany	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Austria	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Belgium	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Switzerland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Luxemburg	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Ireland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Portugal	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Norway	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Denmark	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Finland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Iceland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Greece	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Lichtenstein	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Sweden	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP

Copyright

Copyright 2004 by Acer Inc., All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of Acer Computer GmbH

Disclaimer

Acer Inc. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, Acer Computer GmbH, reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or change.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Contents

1. OVERVIEW	3
1.1 Product Feature.....	3
1.2 System Requirements	3
1.3 Applications	3
2. Installing Your Router	1
2.1 Installation Instructions	1
3. Preparing Your Network.....	2
3.1 Configuring Windows for IP Networking	2
3.2 To Configure Windows to Receive Dynamic IP Address:.....	2
3.3 Collecting ISP Information.....	4
4. Basic Functions	5
4.1 To Open the Web-based Administration Tool:.....	5
4.2 Setup	7
4.3 Global Address	11
4.4. Wireless	14
4.5 Tools	23
4.6 Status	27
4.7 DHCP	30
4.8 Log.....	32
4.9 Statistics.....	35
5. Advanced Function.....	36
5.1. To Toggle between Basic Functions and Advanced Functions:	36
5.2 Virtual Servers	37
5.3 Filters.....	40
5.4 IP/URL Block	44
5.5 Special Apps	47
5.6 DMZ Host.....	51
5.7 MAC Clone	53
5.8 Dynamic DNS	54
5.9 Proxy DNS.....	56
5.10 SNMP	58
5.11 Static Routing	61

1. OVERVIEW

1.1 Product Feature

- Compliance with IEEE 802.11g and 802.11b standards
- Highly efficient design mechanism to provide unbeatable performance
- Strong network security with WEP and 802.1X encryption
- Achieving data rate up to 54Mbps for 802.11g and 11Mbps for 802.11b with wide range coverage; high performance to deliver up to 54Mbps raw data rate for 802.11g
- Quick and easy setup with Web-based management utility

1.2 System Requirements

- Windows 98, 98SE, Millennium Edition (ME), 2000 and XP operating systems
- Microsoft Internet Explorer 5.5 or higher
- DSL/ Cable Modem Broadband Internet connection and ISP account
- PCs equipped with 10 Mbps or 10/100 Mbps Ethernet connection to support TCP/IP protocol
- One CD-ROM driver

1.3 Applications

- Home SOHO networking for device sharing and wireless multimedia
- Wireless office provides a wider range for home and SOHO Ethernet
- Enables wireless building-to-building data communication
- Built-in infrastructure mode
- Router provides ideal solution for:

Temporary LANs for scenarios such as trade-exhibitions and meetings

Enables LAN adaptability to frequently changing environments

Enables remote access to corporate network information, for example e-mail and company home page

2. Installing Your Router

In this chapter, you'll learn how to connect your router.

2.1 Installation Instructions

To Connect the Router:

- 2.1.1.** Make sure all equipments are turned off, including the router, Desktop or Laptop PCs, the cable and DSL modem, and so on.
- 2.1.2.** Connect the WAN Port of the router to the cable and DSL modem, Ethernet Server or the hub.
- 2.1.3.** Connect your client PCs to the LAN Ports.
- 2.1.4.** Connect the Power Adaptor (5VDC, 1.2A) to the power jack of the router and plug the power cable into the outlet.
- 2.1.5.** Turn on our PCs.

3. Preparing Your Network

In this chapter, you'll learn what to do before configuring your network.

Before configuring your router, you need set up the computers in your network for TCP/IP networking and collect relevant ISP information if necessary.

3.1 Configuring Windows for IP Networking

Each computer in your network should be configured for TCP/IP networking. There are two ways to configure your computers:

- You are commended to use DHCP, then you can simply choose to receive an IP address automatically. For detailed instructions, see [Configure Windows to Receive Dynamic IP Address](#).
- If you don't use DHCP, you need assign an IP address to each computer manually. For detailed instructions, refer to your Windows Documentation.

3.2 To Configure Windows to Receive Dynamic IP Address:

3.2.1. Click Start, then choose Settings > Network and Dial-up Connections.

3.2.2. Select the name of your ISP connection.

The Local Area Connection Status dialog box appears, seen in FIGURE 3-1:

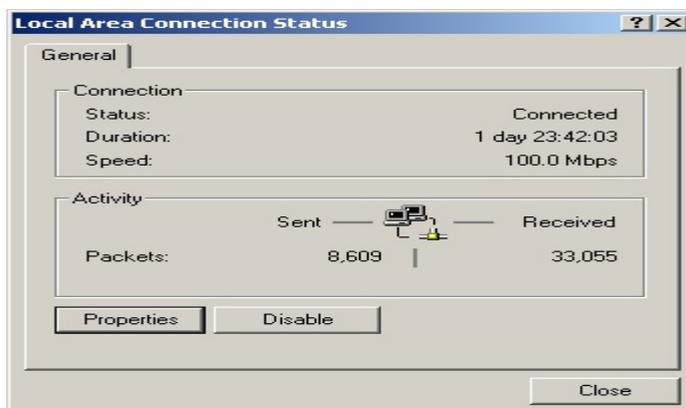


FIGURE 3-1: Local Area Connection Status dialog box

3.2.3. Click Properties.

The Local Area Connection Properties dialog box appears, seen in FIGURE 3-2:

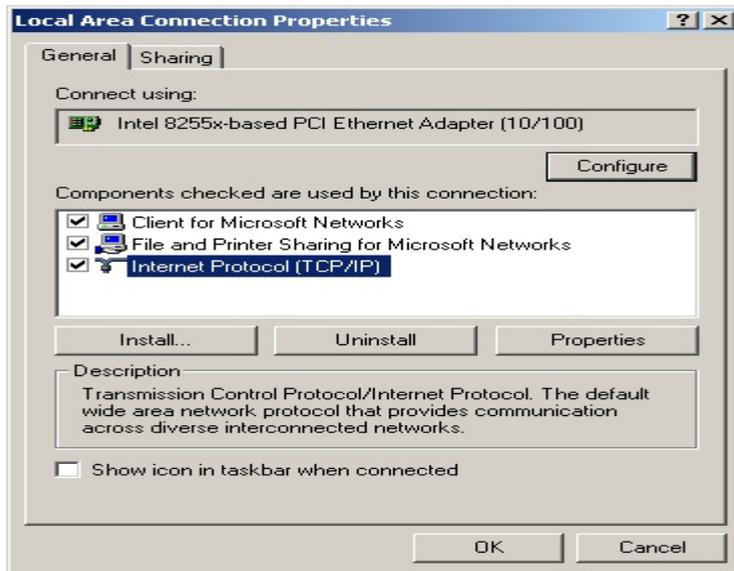


FIGURE 3-2: Local Area Connection Properties dialog box.

3.2.4. Click Internet Protocol (TCP/IP), then click Properties.

The Internet protocol (TCP/IP) Properties dialog box appears, seen in FIGURE 3-3:

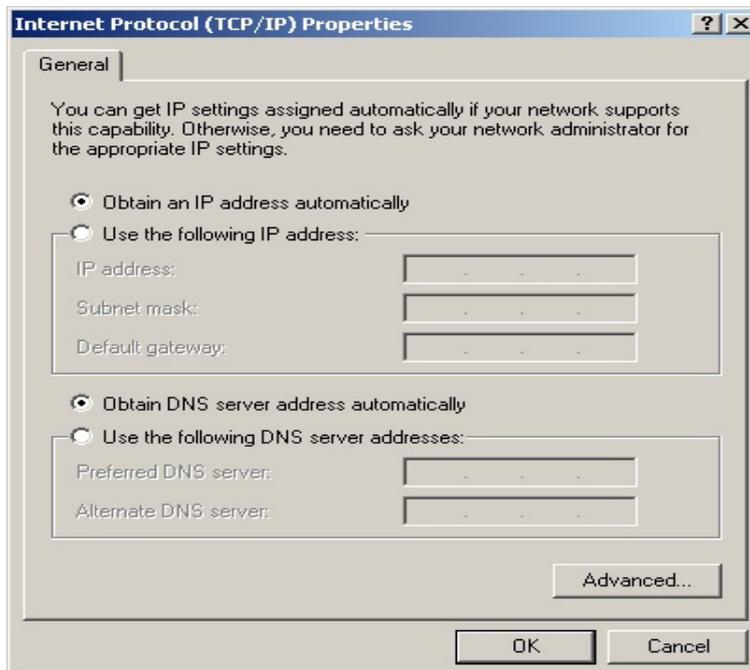


FIGURE 3-3: Internet Protocol (TCP/IP) Properties dialog box

3.2.5. Click Obtain an IP address automatically and Obtain DNS server address automatically.

3.2.6. Click OK.

You need restart your computer now or at a later time.

Note :

The procedural steps above apply to Windows 2000 only. For Windows 95/98/ME/NT/XP, refer to your Windows Documentation.

3.3 Collecting ISP Information

You need query the relevant information from your ISP before configuring your router, for example:

- **Has your ISP assigned you a static or dynamic IP address? If you have obtained one static IP address, what is it?**
- **Does your ISP use PPPoE? If so, what is your PPPoE user name and password?**

If you are not sure of the above questions, call your ISP to clarify them.

4. Basic Functions

In this chapter, you will learn how to use basic functions that the Company AP Router provides, including Setup, Global Address, Wireless Tools, Status, DHCP, Log and Printer.

The Acer WLAN 11g Broadband Router provides you a Web-based Administration Tool with which you can easily set up the router and customize the basic router settings. You can use this Web-based Tool from any computer in your network.

Notes :

Microsoft Internet Explorer 5.0 or later is highly recommended for using this Web-based Tool.

Graphics sampled in this chapter are provided for illustrations only. They may slightly differ from your own router screens.

4.1 To Open the Web-based Administration Tool:

4.1.1. Open the browser on your PC.

4.1.2. Type *http://192.168.62.1* in the Address bar.

The Logon dialog box appears, seen in FIGURE 4-1:



FIGURE 4-1: Logon dialog box

4.1.3. Type *admin* in the User Name box.

4.1.4. Type the password in the box.

Note :

The default password is “1234”. You can change the password on the Tools page. For detailed instructions, see [To Change the Administrative Password for Your Router](#).

4.1.5. Optional. To log on to the Administration Tool once for all, select the check box of Save this password in your password list.

4.1.6. Click OK.

Note :

The Administration Tool will time out after a period of idling, the Router may ask you to log on again.

The Company AP Router Administration Tool appears.

4.2 Setup

The Setup page allows you to edit the basic configuration parameters for your router, such as *Host Name*, *Domain Name*, *LAN IP Address*, *WAN IP Address*, *PPPoE Login*, *UPNP*, and so on.

In most cases, the default settings will be Okay for you. However, different ISPs (Internet Service Provider) may ask for specific requirements, please check it with your ISP if you are not sure.

4.2.1. To Configure Setup Parameters:

4.2.1.1. Click Setup on the navigation bar.

The Setup page appears, seen in FIGURE 4-2:

The screenshot shows a web-based configuration interface for a router. On the left is a blue vertical sidebar with labels for various settings. The main area contains the corresponding configuration fields and options.

Host Name:	<input type="text"/>	(Required by some ISPs)
Domain Name:	<input type="text"/>	(Required by some ISPs)
Firmware Version:	20-06-07, Oct 20 2003 17:09:22	
Time:	Thu Nov 6 3:52:57 2003	
Set Time Zone:	[(GMT-08:00)Pacific Time (US&Canada):Tijuana]	
Daylight Savings:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Daylight Period:	[JAN] [01] ~ [JAN] [01]	
LAN IP Address:	Device IP Address: [192] . [168] . [62] . [1] Subnet Mask: [255] . [255] . [255] . [0]	
WAN IP Address:	<input checked="" type="radio"/> Obtain an IP Address Automatically <input type="radio"/> Specify an IP Address WAN IP Address: [0] . [0] . [0] . [0] Subnet Mask: [0] . [0] . [0] . [0] ISP Gateway Address: [0] . [0] . [0] . [0] DNS 1: [0] . [0] . [0] . [0] 2: [0] . [0] . [0] . [0] 3: [0] . [0] . [0] . [0]	
PPPoE Login:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable User Name: [ad50189026] Password: [*****] <input type="radio"/> Connect on Demand <input checked="" type="radio"/> Connect Manually <input checked="" type="checkbox"/> Max Idle Time [10] Minutes	
UPNP:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
[Apply] [Cancel] [Help]		

FIGURE 4-2: Setup page

4.2.1.2. Type the Host Name, System Name or Account Name in the Host Name box if your ISP requires.

- 4.2.1.3. Type the Domain Name of your ISP in the box if your ISP requires, such as *xyz.isp.com*.
- 4.2.1.4. Optional. Review the firmware version number and date information that you are currently using.
- 4.2.1.5. Select a specific Time Zone from the Set Time Zone drop-down list, such as *(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi*.
- 4.2.1.6. If you want to use Daylight Savings time, click Enable and select the start date and end date from the Daylight Period drop-down lists.
- 4.2.1.7. If you don't want to use Daylight Savings time, click Disable. If you select to disable the Daylight Savings, Daylight Period will not take effect any more.
- 4.2.1.8. Optional. Review the Device IP Address and Subnet Mask next to LAN IP Address and change the information if necessary.

LAN IP Address:	Device IP Address:	<input type="text" value="192"/>	.	<input type="text" value="168"/>	.	<input type="text" value="62"/>	.	<input type="text" value="1"/>
	Subnet Mask:	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="0"/>

Notes :

Device IP Address and Subnet Mask are invisible to users on the LAN (Local Area Network) only.

In most cases, you need not make any change to LAN IP Address. If you change the LAN IP Address with DHCP enabled, you need to restart your client PCs; otherwise, you need reconfigure your client's IP addresses manually.

- 4.2.1.9. If you have enabled the DMZ feature on the DHCP page, review the DMZ IP Address and Subnet Address next to DMZ IP Address and change the information if necessary.
- 4.2.1.10. For WAN IP Address (Wide Area Network, also called Public IP), choose either Obtain an IP Address automatically or Specify an IP Address if your ISP has assigned you with static IP).

Note :

If you choose to obtain an IP Address automatically, skip Step

- 4.2.1.11. Optional. If you select Specify an IP Address, type the WAN IP Address, Subnet Mask, ISP Gateway Address and DNS in

the boxes, seen in FIGURE 4-3. You can collect such information from your ISP.

Specify an IP Address

WAN IP Address: . . .

Subnet Mask: . . .

ISP Gateway Address: . . .

DNS

1: . . .

2: . . .

3: . . .

FIGURE 4-3: WAN IP Address - Specify an IP Address

4.2.1.12. If your ISP uses PPPoE (Point to Point Protocol over Ethernet), click Enable next to PPPoE Login; otherwise, click Disable. For detailed instructions on how to set the PPPoE Login parameters in FIGURE 3-4, see [To Set PPPoE Login Parameters](#) below.

Notes :
Using PPPoE, your ISP can authenticate your connection with a specific user name and password for security issues.
If you enable PPPoE, make sure to uninstall all existing applications on any computer in your network.

4.2.1.13. If you want to use UPNP (Universal Plug and Play) to plug devices like PCs, routers and others into a network and to automatically know about each other, click Enable next to UPNP; otherwise, click Disable.

4.2.1.14. When you have completed all the settings, click Apply, or click Cancel to undo your changes.

4.2.2. To Set PPPoE Login Parameters:

4.2.2.1. Click Enable next to PPPoE Login.

PPPoE Login: Enable Disable

User Name:

Password:

Connect on Demand Connect Manually

Max Idle Time Minutes

FIGURE 4-4: Set PPPoE Login Parameters

- 4.2.2.2.** Type the User Name and Password provided by your ISP.
- 4.2.2.3.** For connection types, you can select either Connect on Demand or Connect Manually.
- 4.2.2.4.** Optional. If you want to limit the idling minutes, select Max Idle Time and type a maximum number in minutes.

4.3 Global Address

On the Global Address page, you can set up NAT (Network Address Translation) to provide internal-to-external IP address mappings.

Notes :

If you want to use Global Address mapping, you must enable NAT on the Filters page. For detailed instructions, see [To Set up a Port Filtering or Raw IP Filter](#).

If you have chosen to retrieve an IP address automatically, you will not need to use this function. Instead, the default public IP address will display on the Global Address page.

Have you enabled DMZ on the DHCP page? Depending on whether DMZ is enabled, you may follow different procedural steps.

What do you want to do?

- [Set up Global Address with DMZ Disabled](#)
- [Set up Global Address with DMZ Enabled](#)
- [Remove Global Addresses](#)

4.3.1. To Set up Global Address with DMZ Disabled:

4.3.1.1. Click Global Address on the navigation bar.

The Global Address page with DMZ Disabled appears, seen in FIGURE 4-5:

Setup	Global Address	Wireless	Tools	Status	DHCP	Log	Statistics
1: 0.0.0.0 (default public IP)							
2: [0] . [0] . [0] . [0]							
3: [0] . [0] . [0] . [0]							
4: [0] . [0] . [0] . [0]							
5: [0] . [0] . [0] . [0]							
6: [0] . [0] . [0] . [0]							
7: [0] . [0] . [0] . [0]							
8: [0] . [0] . [0] . [0]							
[Apply] [Cancel] [Help]							

FIGURE 4-5: Global Address Page with DMZ Disabled

4.3.1.2. Review the first line in the above figure. It shows the default WAN IP address which is specified on the Setup page. If your

ISP assigns you an IP address automatically, it will display here.

4.3.1.3. In Line 2 – Line 8, you can list up to 7 additional static, external IP addresses provided by your ISP.

4.3.1.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.3.2. To Set up Global Address with DMZ Enabled:

4.3.2.1. Click Global Address on the navigation bar.

The Global Address page with DMZ Enabled appears, seen in **FIGURE 4-6:**

Setup	Global Address	Wireless	Tools	Status	DHCP	Log	Statistics
External-Internal							
1	200	168	76	2			
2	0	0	0	0			
3	0	0	0	0			
4	0	0	0	0			
5	0	0	0	0			
6	0	0	0	0			
External-DMZ							
1	0	0	0	0			
2	0	0	0	0			
3	0	0	0	0			
4	0	0	0	0			
5	0	0	0	0			
6	0	0	0	0			
Apply Cancel Help							

FIGURE 4-6: Global Address Page with DMZ Enabled

4.3.2.2. Review the first line in the above figure. It shows the default WAN IP address which is specified on the Setup page. If your ISP assigns you an IP address automatically, it will display here.

4.3.2.3. Next to External - Internal, you can list up to 6 static, external IP addresses provided by your ISP.

4.3.2.4. Next to External – DMZ, define for your DMZ network up to 6 static, external global IP addresses provided by your ISP.

4.3.2.5. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.3.3. To Remove Global Addresses:

4.3.3.1. Click Global Address on the navigation bar.

4.3.3.2. For any entry you want to delete, enter *0.0.0.0*, and click Apply.

4.4. Wireless

Using Wireless, you can configure your router for wireless access. There are three parts on the Wireless page:

- **Radio Settings:** Allows you to configure your Gateway for wireless access, including *Wireless Enable/Disable, Mode, ESSID, Beacon Interval, RTS Threshold, Preamble Type, Distribution System*, and so on.
- **Security Setting:** Allows you to configure your Gateway for security issues.
- **Status:** Allows you to find out your Gateway's AP Radio statistics and wireless devices of which the AP (Access Point) is aware.

You can easily toggle between the above three parts on the Wireless page.

On the Radio Settings page, Wireless Distribution System as defined by the IEEE 802.11 standard has been made available on the Company AP Router now. Hence, it is possible to wirelessly connect Access Points using up to 8 MAC Addresses of PC cards, so that you can extend a wired infrastructure to locations where cabling is not available. Thus those users can roam or stay connected to the available network resources.

What do you want to do?

- Set the Wireless Radio Parameters
- Set the Wireless Security Parameters
- Review Wireless Status
- Disable Wireless

4.4.1. To Set the Wireless Radio Parameters:

4.4.1.1. On the Wireless page, select Radio Settings.

The Radio Settings page appears, seen in FIGURE 4-7:

FIGURE 4-7: Wireless – Radio Settings Page

4.4.1.2. Click Enable next to Wireless.

4.4.1.3. Optional. Review the firmware version number and date information that you are currently using.

4.4.1.4. Enter the following basic radio parameters:

Parameter	Description
Mode	<p>Selects the Wireless Mode that your Company AP Router supports from the drop-down list.</p> <p>Available options are <i>802.11B</i>, <i>802.11G</i>, and <i>MIXED</i> which supports both 802.11B and 802.11G.</p>
ESSID	<p>Type the unique identifier for the Extended Service Set which is shared by client stations in an infrastructure association, such as <i>WLAN-test</i>.</p> <p>It is case-sensitive and cannot exceed 32 characters.</p>
Channel	<p>Selects one IEEE 802.11G channel for wireless LAN transmissions from the drop-down list.</p> <p>Specifies the bandwidth which the wireless radio operates. AP and the client stations that is</p>

	associated work in one of channels from 1 to 14.
--	--

4.4.1.5. Enter the following advanced radio parameters:

Parameter	Description
Beacon Interval	Type the time interval in milliseconds between beacons broadcast by AP (Access Point) in the Beacon Interval box, such as 100.
RTS Threshold	Type a number in the RTS Threshold box. Also called Request-to-Send Threshold. This field specifies the minimum size of data frames above which RTS protocol is used, ranging from 256 to 2432. RTS helps prevent data collision from hidden nodes.
Fragmentation Threshold	Type a number in the Fragmentation Threshold box. For efficiency in high-traffic situations, large files are split into fragments. This field specifies the default packet size, an even number ranging from 256 to 2346.
DTIM Interval	Type a number in the DTIM Interval box. Also called Delivery Traffic Indication Map. This field specifies the number of beacon intervals between successive DTIMs, ranging from 1 to 255.
Preamble Type	Select either Short Preamble (72 bits) or Long Preamble (144 bits).
Distribution System	If you want to use Wireless Distribution System on your Router, click Enable next to Distribution System, then type the distributed client PCs' physical addresses, as described in Step 6. Otherwise, click Disable.

<p>Note : You can see the default values of the above advanced wireless settings on the right of the page. If you don't know how to change the settings, please leave as they are in Figure 4-8:</p>

Default Values for Radio Settings	
Beacon Interval	100
RTS Threshold	2432
Fragmentation Threshold	2346
DTIM Interval	1
Preamble Type	Long Preamble
Distribution System	Disable

FIGURE 4-8: Default Values for Radio Settings

4.4.1.6. Optional. If you have enabled Distribution System, type the physical addresses of distributed client PCs in a wireless network in the Peer AP MAC Address 1-8 boxes, seen in FIGURE 4-9:

Distribution System:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Peer AP MAC Address 1:	<input type="text"/>
Peer AP MAC Address 2:	<input type="text"/>
Peer AP MAC Address 3:	<input type="text"/>
Peer AP MAC Address 4:	<input type="text"/>
Peer AP MAC Address 5:	<input type="text"/>
Peer AP MAC Address 6:	<input type="text"/>
Peer AP MAC Address 7:	<input type="text"/>
Peer AP MAC Address 8:	<input type="text"/>

FIGURE 4-9: Peer AP MAC Addresses for Distribution Systems

4.4.1.7. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.4.2. To Set Wireless Security Parameters:

4.4.2.1. Click Security Settings on the Wireless page.

The Security Settings appears, seen in FIGURE 4-10:

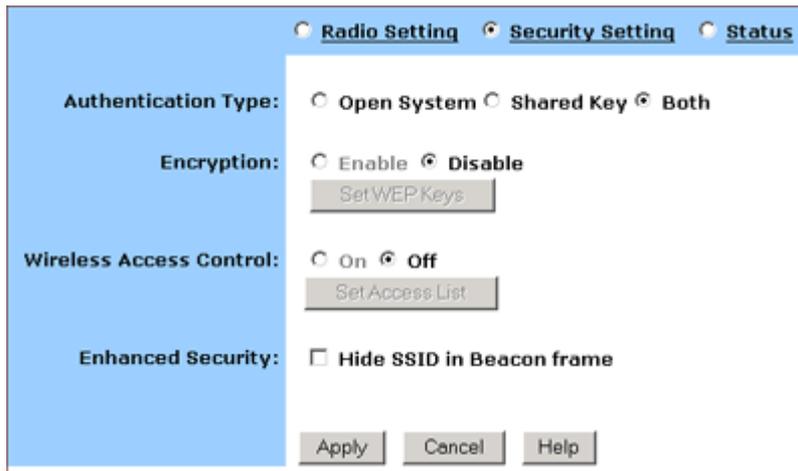


FIGURE 4-10: Wireless – Security Settings Page

4.4.2.2. Select one of *Open System*, *Shared Key* and *Both* from the Authentication Type drop-down list.

Notes :

Authentication Type indicates an authentication algorithm which can be supported by the Access Point:

Open System: The simplest of available authentication algorithms. Essentially it is a null algorithm. Any station that requests authentication with this algorithm may become authenticated if Open System is set at the recipient station.

Shared Key: Allows stations with a specific WEP (Wired Equivalent Privacy) Keys to be authenticated.

Both: Supports the authentications of either stations who know a shared key or those who do not.

If you want to prevent other stations without specific WEP (Wired Equivalent Privacy) keys from linking to the AP, select Enable next to Encryption and then click Set WEP Keys to specify relevant keys; otherwise, select Disable. For detailed instructions on how to set the WEP Keys, see below To Set WEP Keys.

If you want to allow access to the Internet based on user’s MAC (Media Access Control) address, select On next to Wireless Access Control and then click Set Access List to specify relevant MAC addresses; otherwise, click Off. For detailed instructions on how to specify relevant MAC addresses, see below To Set Wireless Access Control.

4.4.2.3. Next to Enhanced Security, select either Enable or Disable. If you choose to enable the enhanced security feature, go to Step 6.

4.4.2.4. Optional. If you have enabled Enhanced Security, you can choose to hide your SSID (Service Set Identifier) in Beacon frame.

4.4.2.5. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.4.3. To Set WEP Keys:

4.4.3.1. On the Security Settings page, enable the Encryption and click Set WEP Keys.

The Set WEP Keys window appears, seen in FIGURE 4-11:

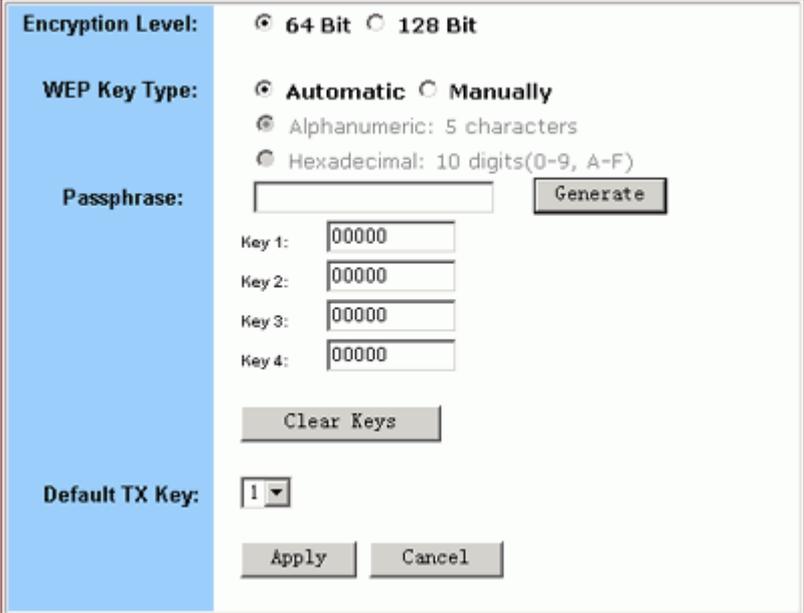


FIGURE 4-11: Set WEP Keys Window

4.4.3.2. Select either *64 Bit* or *128 Bit* next to Encryption Level.

Note :

128 Bit encryption can provide you a more secure encryption algorithm, but it will slow down your network data transmission rates.

4.4.3.3. If you want to generate WEP Keys automatically, do the following action:

4.4.3.3.1. Select Automatic next to WEP Key Type.

4.4.3.3.2. Type a string of any words in the Passphrase box, and click Generate.

Four newly generated WEP Keys will display in the Key 1 – Key 4.

4.4.3.3.3. Optional. Click Clear Keys to reset all the keys to null.

Note :

Make sure that you write down the passphrase string, so that you can refer to it if necessary.

4.4.3.4. If you want to enter the key elements manually, do the following action:

4.4.3.4.1. Select Manually next to WEP Key Type.

4.4.3.4.2. If you select Alphanumeric: 5 characters, type a string of 5 alphanumeric characters in the Key 1 – Key 4 boxes respectively.

4.4.3.4.3. If you select Hexadecimal: 10 digits (0-9, A-F), type a string of 10 hexadecimal digits in the Key 1 – Key 4 boxes respectively.

4.4.3.4.4. Optional. Click Clear Keys to reset all the keys to null.

4.4.3.5. Select the default encryption key from the Default TX Key drop-down list, such as Key 1.

4.4.3.6. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.4.4. To Set Wireless Access Control:

4.4.4.1. On the Security Settings page, set the Wireless Access Control On and click Set Access List.

The Window Control List window appears, seen in FIGURE 4-12:

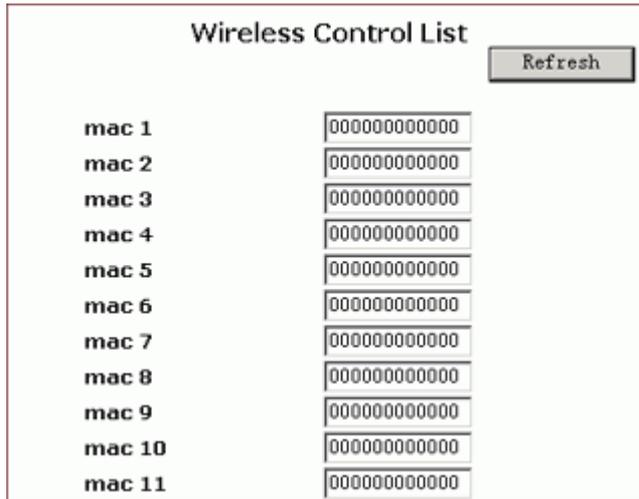


FIGURE 4-12: Wireless Control List window

- 4.4.4.2. Type the MAC addresses that you want to allow to access the Internet. You can specify up to 80 MAC addresses in the list.
- 4.4.4.3. When you have complete editing all the MAC addresses, click Submit, or click Cancel to undo your changes.
- 4.4.4.4. Optional. You can click Refresh to see the most current MAC addresses in effect.

4.4.5. To Review Wireless Status:

- 4.4.5.1. On the Wireless page, select Status.

The Status page appears with your GateWay’s AP Radio statistics including *Status*, *Max.Mb/s*, *IP Addr*, *MAC Addr*, *Radio SSID*, *Receive data* and *Transmit data*. Seen in FIGURE 4-13:

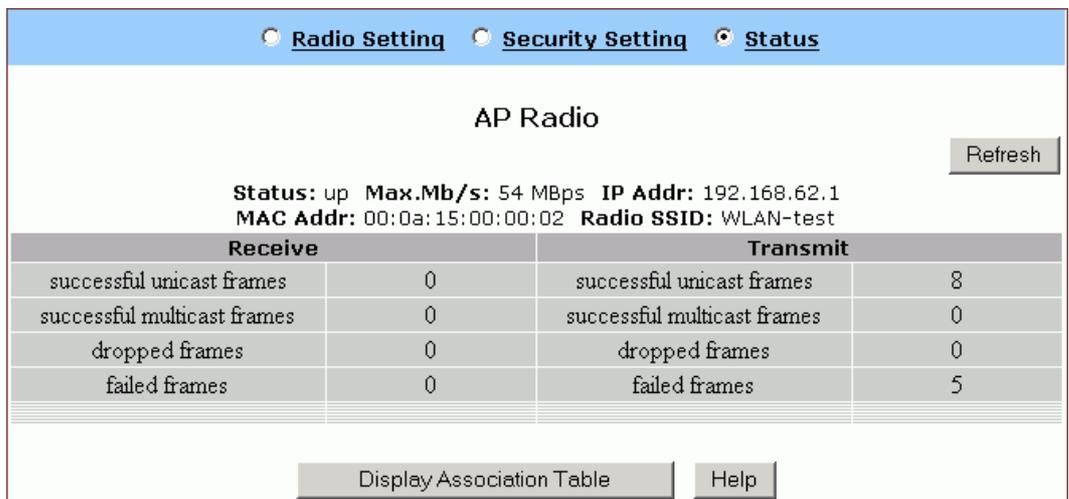


FIGURE 4-13: Wireless – Status Page

4.4.5.2. To see the wireless devices of which the AP (Access Point) is aware, click Display Association Table.

Wireless Association Table			
Index	Time	Mac Address	Add/Delete from Access List
1	None	None	None

4.4.5.3. Optional. You can click Refresh to see the most current data.

4.4.6. To Disable Wireless:

4.4.6.1. On the Wireless page, select Radio Settings.

The Radio Settings page appears, seen in FIGURE 4-7.

If you don't want the router to support Wireless, select Disable.

Note :
None of the router's wireless functions will work unless you enable it.

4.5 Tools

On the Tools page, you can:

- [Change the Administrative Password for Your Router](#)
- [Restore the Factory Default Configuration](#)
- [Reset Gateway](#)
- [Upgrade the Firmware](#)

! Important:

We strongly recommend that you change the administrative password after the first login.

Restoring the default factory settings will reset all of the router configurations in every page, so we recommend that you backup the configuration data from the Gateway to your PC simply using DOS commands. In addition, you can also restore the factory defaults under the DOS window. For detailed instructions, see [To Backup or Restore the Configuration Data Using DOS Commands](#).

If you want to reset the hardware, you need reset the Gateway. Before upgrading the firmware, you need download the firmware image file from the Gateway Web site and save it to your root local drive first.

4.5.1. To Change the Administrative Password for Your Router:

4.5.1.1. Click Tools on the navigation bar.

The Tools page appears, seen in FIGURE 4-14:

The screenshot shows a web interface with a blue sidebar on the left containing the following menu items: "Change Password:", "Restore Factory Defaults:", "Reset Gateway:", and "Upgrade Firmware:". The main content area contains the following elements:

- Change Password:** Three input fields for "Old Password:", "New Password:", and "Confirm Password:". Below the "New Password:" field is the text "(* Maximum 31 characters)". Below the input fields are three buttons: "Apply", "Cancel", and "Help".
- Restore Factory Defaults:** Two buttons: "Restore to Default" and "Backup/Restore Help".
- Reset Gateway:** One button: "Reset".
- Upgrade Firmware:** One input field, one "Browse..." button, one "Upgrade now" button, and one "Help" button.

FIGURE 4-14: Tools Page

4.5.1.2. Type the Old Password in the box. The default password is 1234.

4.5.1.3. Type a New Password in the box.

Note :
Password must be less than 64 characters.

4.5.1.4. Type the new password in the Confirm Password box.

4.5.2. To Restore the Factory Default Configuration:

4.5.2.1. On the Tools page, click Restore to Default next to Restore Factory Defaults.

The Warning dialog box appears, see FIGURE 4-15:



FIGURE 4-15: Warning Dialog Box

4.5.2.2. Click OK.

Important:
Restoring the default factory settings will reset all of the router configurations in every page, so we recommend that you backup the configuration data from the Gateway to your PC first using DOS commands. For details, see To Backup or Restore the Configuration Data Using DOS Commands.
In addition, you can also restore the factory defaults using DOS commands. For detailed instructions, see To Backup or Restore the Configuration Data Using DOS Commands.

4.5.3. To Backup or Restore the Configuration Data Using DOS Commands:

For the backup of the configuration data from the Gateway to your PC, Gateway acts as a TFTP server.

To backup the configuration data, under the DOS window, use the following command:

```
tftp -i gateway_Ip_address GET filename
```

To restore the configuration data, under the DOS window, use the following command:

```
tftp -i gateway_ip_address PUT filename
```

gateway_ip_address: The IP address of the Gateway where you want to back the configuration data.

filename: The file name for backup from the Gateway. It must begin with “*nvr*am” which is not case-sensitive, such as “*nvr*am__11032003”.

4.5.4. To Reset Gateway:

If you want to reset the hardware, click **Reset** next to **Reset Gateway** on the **Tools** page.

4.5.5. To Upgrade the Firmware:

4.5.5.1. Download a firmware image file from the Gateway Web site and save it to your root local drive.

4.5.5.2. Type the file path and file name in the Upgrade Firmware box, or click **Browse** to launch a Choose file dialog box, seen in FIGURE 4-15:

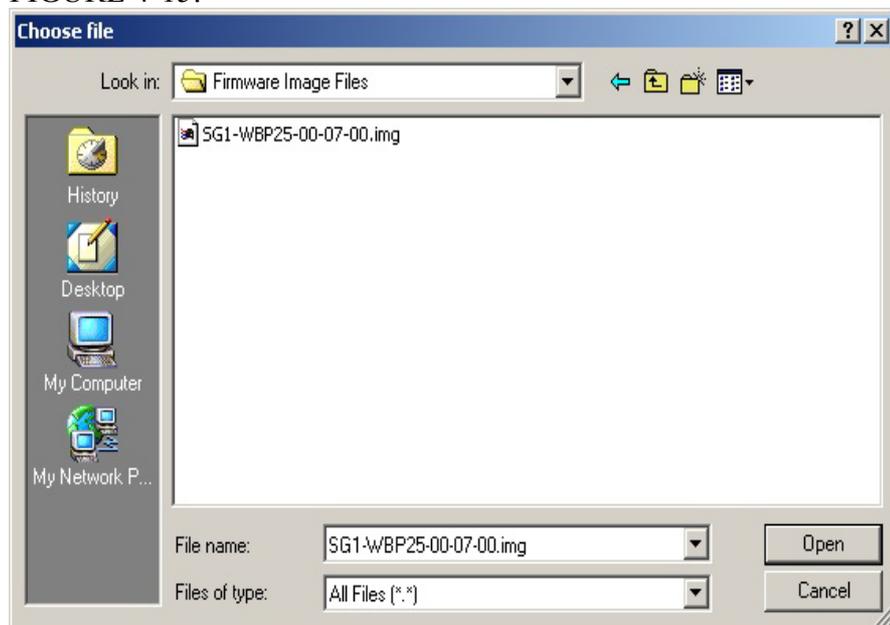


FIGURE 4-15: Choose File Dialog Box for Upgrading Firmware

4.5.5.3. Locate the firmware you have downloaded and click **Open**.

4.5.5.4. The Choose file dialog box closes.

4.5.5.5. Click Upgrade Now. The firmware of the device will be

Caution :

The firmware upgrade may take about 10 seconds, please DONOT power off the unit when it is being upgraded.

upgraded.

4.6 Status

On the Status page, you can view the most current information about your Router which will be continuously refreshed per 10 seconds, such as *Host Name, Domain, PPPoE Login, LAN/WAN* and *DDNS Status*. Different configuration may bring you to different data, compared in FIGURE 3-16 and FIGURE 4-17.

Note :

If you want to change the configuration, go to the Setup page. For detailed instructions, see [Setup](#).

- If you have enabled the PPPoE Login, the Status page will display as illustrated in FIGURE 4-16:

Host Name:	StartGate
Domain:	xyz.isp.com
PPPoE Login:	Enabled Status: Disconnected
	<input type="button" value="Connect"/>
LAN:	
	IP Address: 192.168.62.1
	Subnet Mask: 255.255.255.0
WAN:	Dynamic
	IP Address: 0.0.0.0
	Subnet Mask: 255.0.0.0
	Default Gateway: 255.255.255.255
	DNS: 0.0.0.0 0.0.0.0 0.0.0.0
DDNS Status:	
	Server: The service is disabled
	Status: The account is not set yet.
	<input type="button" value="Help"/>

FIGURE 4-16: Status Page with PPPoE Login Enabled

- If you have chosen the Dynamic IP and disabled PPPoE Login, the Status page will display as illustrated in FIGURE 4-17:

▪

Host Name:	StartGate	
Domain:	xyz.isp.com	
PPPoE Login:	Disabled	
LAN:		
	IP Address:	192.168.62.1
	Subnet Mask:	255.255.255.0
WAN:	Dynamic	
	IP Address:	0.0.0.0
	Subnet Mask:	255.0.0.0
	Default Gateway:	255.255.255.255
	DNS:	0.0.0.0
		0.0.0.0
		0.0.0.0
	<input type="button" value="DHCP Release"/>	<input type="button" value="DHCP Renew"/>
DDNS Status:		
	Server:	The service is disabled
	Status:	The account is not set yet.
	<input type="button" value="Help"/>	

FIGURE 4-17: Status Page with PPPoE Login Disabled

Notes :

**If you have chosen the Dynamic IP and disabled PPPoE Login, you can see the DHCP Release and DHCP Renew buttons:
To release the most current WAN IP address, click DHCP Release.
To renew the WAP IP address, click DHCP Renew.**

Status Detail:

Parameter	Description
Host Name	Shows the name of the device.
Domain	Shows the domain name of the device.
PPPoE Login	Shows the current status of PPPoE Login: <ul style="list-style-type: none"> ▪ Disabled ▪ Enabled: Connected, Connecting or Disconnected.
LAN	Shows the current IP Address and Subnet Mask of the device, as seen by users in your internal network.
WAN	Shows the IP Address, Subnet Mask, Default Gateway, and DNS of the router, as seen by

	external users on the Internet.
DDNS	Shows the Dynamic DNS Server and Status. If you want to change the setting, go to the Advanced Dynamic DNS page. For details instructions, see <u>To Configure a Dynamic DNS Server</u>.

4.7 DHCP

On the DHCP page, you can set your NAT/Firewall Gateway as a DHCP (Dynamic Host Configuration Protocol) server, and DHCP servers will automatically assign IP addresses to all the client PCs in your network.

Notes

If you want to enable DHCP, make sure that there is not already a DHCP server on your router.

If you don't enable DHCP on your router, you will need to manually configure an IP address for each PC in your network; if you do enable DHCP, make sure that each PC is configured to receive an IP address automatically.

What do you want to do then?

- Set Your Router as a DHCP Server
- View the Active IP Table
- Disable DHCP on Your Router

4.7.1. To Set Your Router as a DHCP Server:

4.7.1.1. Make sure that there is not already a DHCP server on your router.

4.7.1.2. Make sure that each PC in your network is configured to receive an IP address automatically.

4.7.1.3. Click DHCP on the navigation bar.

The DHCP page appears, seen in FIGURE 4-18:

DHCP Server: Enable Disable
IP Pool Starting Address: 192.168.62.50
IP Pool Ending Address: 192.168.62.100
Lease Time: 24 Hours.
Display DHCP Table
Apply Cancel Help

FIGURE 4-18: DHCP Page

4.7.1.4. Click Enable next to DHCP Server.

- 4.7.1.5. Type a IP Pool Starting Address to designate the first IP address that can be assigned to a PC in your network.
- 4.7.1.6. Type a IP Pool Ending Address to designate the last IP address that can be assigned to a PC in your network.
- 4.7.1.7. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.7.2. To Disable DHCP on Your Router:

- 4.7.2.1. On the DHCP page, click Disabled next to DHCP Server.
- 4.7.2.2. Click Apply.

4.7.3 To View the Active IP Table:

If you want to find out the information about PCs that have been assigned IP addresses by the DHCP server, click Display DHCP Table.

DHCP Server IP Address, Client Host Name, IP Address and MAC Address for each active client PC will be listed out in the table, seen in FIGURE 4-19:

DHCP Active IP Table			
DHCP Server IP Address:			192.168.62.1
Index	Client Host Name	IP Address	MAC Address
1	swlab2	192.168.62.51	00:06:5b:a5:7b:59

FIGURE 4-19: DHCP Active IP Table

Optional. Click Refresh to obtain the most current data.

Note :

If you have enabled the DMZ and LAN features, you can also find the relevant information in the DHCP Active IP Table for DMZ Zone and the DHCP Active IP Table for LAN.

4.8 Log

On the Log page, you can set up Access Log and view log files that record the access activity of LAN and WAN client PCs, including *Session Event Log*, *Block Event Log*, *Intrusion Event Log* and *Wireless Event Log*.

What do you want to do?

- [Set up Access Log on Your Router](#)
- [View Session Event Log](#)
- [View Block Event Log](#)
- [View Intrusion Event Log](#)
- [View Wireless Event Log](#)

4.8.1. To Set up Access Log on Your Router:

4.8.1.1. Click Log on the navigation bar.

The Log page appears, seen in FIGURE 4-20:

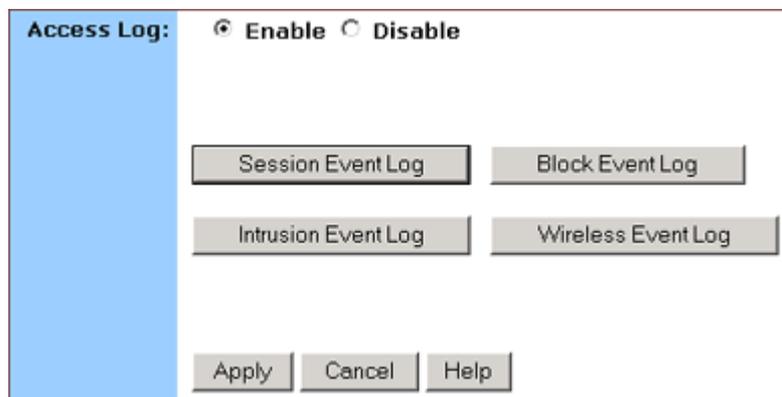


FIGURE 4-20: Log Page

4.8.1.2. Select Enable.

4.8.1.3. Click Apply, or click Cancel to undo your changes.

4.8.2. To View Session Event Log:

4.8.2.1. Click Session Event Log on the Log page.

The Session Event Log Table appears, including each session event entry information like *Record Name*, *Transport type*, *Source IP* and so on, seen in FIGURE 4-21:

Session Event Log Table							
Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2003.11.06 03:34:22	ICMP	61.173.63.220	0:8	61.171.242.88	0:0	POLICY_MIGRATION
2	2003.11.06 03:34:45	ICMP	218.80.56.153	0:8	61.171.242.88	0:0	POLICY_MIGRATION
3	2003.11.06 03:34:38	UDP	61.171.242.88	123	192.5.41.40	123	POLICY_MIGRATION
4	2003.11.06 03:35:49	ICMP	61.172.27.50	0:8	61.171.242.88	0:0	TIMBOUT
5	2003.11.06 03:36:41	ICMP	61.172.104.82	0:8	61.171.242.88	0:0	TIMBOUT

FIGURE 4-21: Session Event Log Table

4.8.2.2. Optional. Click Refresh to obtain the most current data.

4.8.2.3. Optional. Click Clear to delete all the log information.

4.8.3. To View Block Event Log:

4.8.3.1. Click Block Event Log on the Log page.

The Block Event Log Table appears, including each block event entry information like *Record Name*, *Transport type*, *Source IP* and so on, seen in FIGURE 4-22:

Block Event Log Table							
Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2003.11.06 03:34:46	TCP	218.80.56.153	3820	61.171.242.88	135	Default Defense
2	2003.11.06 03:34:52	TCP	218.80.56.153	3820	61.171.242.88	135	Default Defense
3	2003.11.06 03:35:01	TCP	61.171.212.54	3196	61.171.242.88	445	Default Defense
4	2003.11.06 03:35:04	TCP	61.171.212.54	3196	61.171.242.88	445	Default Defense
5	2003.11.06 03:36:00	TCP	195.117.228.35	4066	61.171.242.88	2098	Default Defense

FIGURE 4-22: Block Event Log Table

4.8.3.2. Optional. Click Refresh to obtain the most current data.

4.8.3.3. Optional. Click Clear to delete all the log information.

4.8.4. To View Intrusion Event Log:

4.8.4.1. Click Intrusion Event Log on the Log page.

The Intrusion Event Log Table appears, including each intrusion event entry's *Record Name* and *Intrusion Type*, seen in FIGURE 4-23:

Intrusion Event Log Table		
		<input type="button" value="Clear"/> <input type="button" value="Refresh"/>
Index	Record Time	Intrusion Type
1	None	None

FIGURE 4-23: Intrusion Event Log Table

4.8.4.2. Optional. Click Refresh to obtain the most current data.

4.8.4.3. Optional. Click Clear to delete all the log information.

4.8.5. To View Wireless Event Log:

4.8.5.1. Click Wireless Event Log on the Log page.

The Session Event Log Table appears, including each wireless event entry's *Time*, *Severity* and *Description*, seen in FIGURE 4-24:

Wireless Event Log Table			
			<input type="button" value="Refresh"/>
Index	Time	Severity	Description
1	2003.11.06 03:33:10	Info	WLAN zone information is not set
2	2003.11.06 03:33:11	Info	WLAN Access Point started
3	2003.11.06 03:49:42	Info	WLAN zone information is not set
4	2003.11.06 03:49:42	Info	WLAN Access Point started
5	2003.11.06 03:50:42	Info	WLAN zone information is not set
6	2003.11.06 03:50:42	Info	WLAN Access Point started
7	2003.11.06 03:51:42	Info	WLAN zone information is not set
8	2003.11.06 03:51:42	Info	WLAN Access Point started
9	2003.11.06 03:52:12	Info	WLAN zone information is not set
10	2003.11.06 03:52:12	Info	WLAN Access Point started

FIGURE 4-24: Wireless Event Log Table

4.8.5.2. Optional. Click Refresh to obtain the most current data.

4.8.5.3. Optional. Click Clear to delete all the log information.

4.8.6. To Disable Access Log on Your Router:

4.8.6.1. On the Log page, click Disabled next to Access Log.

4.8.6.2. Click Apply.

4.9 Statistics

On the Statistics page, you can view the statistics information of LAN, WAN and AP (Access Point) Radio ports, including *Status*, *Max.Mb/s*, *IP Addr* and *MAC Addr*, *Receive data* and *Transmit data*.

You can click Statistics on the navigation bar, and then the Statistics page appears, seen in FIGURE 4-25:

LAN WAN AP			
LAN Statistics			
Refresh			
Status: up Max.Mb/s: 100.0 IP Addr: 192.168.62.1 MAC Addr: 00:0a:15:00:00:00			
Receive		Transmit	
total bytes	180771	total bytes	2673637
unicast pkts	4542	unicast pkts	2001
multicast pkts	160	multicast pkts	1764
discards	0	discards	0
errors	0	errors	0
unknown protocols	901	packets queued	0
WAN Statistics			
Refresh			
Status: up Max.Mb/s: 100.0 IP Addr: 0.0.0.0 MAC Addr: 00:0a:15:00:00:01			
Receive		Transmit	
total bytes	0	total bytes	1800
unicast pkts	0	unicast pkts	0
multicast pkts	0	multicast pkts	30
discards	0	discards	0
errors	0	errors	0
unknown protocols	0	packets queued	0
AP Radio			
Refresh			
Status: up Max.Mb/s: 54 Mbps IP Addr: 192.168.62.1 MAC Addr: 00:0a:15:00:00:02 Radio SSID: WLAN-test			
Receive		Transmit	
successful unicast frames	0	successful unicast frames	9
successful multicast frames	0	successful multicast frames	0
dropped frames	0	dropped frames	0
failed frames	0	failed frames	3

FIGURE 4-25: Statistics Page

4.9.1. The Statistics page includes three parts:

4.9.1.1. LAN Statistics: Lists out the data on the LAN port.

4.9.1.2. WAN Statistics: Lists out the data on the WAN port.

4.9.1.3. AP Radio: Lists out the data on the Access Point's radio.

Note :

You can also click Refresh in any part above to obtain the most current data.

5. Advanced Function

In this chapter, you will learn how to use the advanced administrative functions that the Company AP Router provides, including Virtual Server, Filters, IP/URL Block, Special Apps, DMZ Host, MAC Clone, Dynamic DNS, Proxy DNS and SNMP.

The Web-based Administration Tool provides you some advanced services on the Advanced Function navigation bar, such as Filtering and cloning your MAC addresses.

In most cases, basic functions are Okay. If you want to set the advanced configuration, you will need to toggle to the Advanced Function navigation bar first.

5.1. To Toggle between Basic Functions and Advanced Functions:

5.1.1. To toggle to the Advanced window, click Advanced on the right side of the Basic window, seen in FIGURE 5-1:



FIGURE 5-1: Advanced Button on the Basic Window

5.1.2. Once you are already in the Advanced window, click Basic on the right side of the Advanced window to return to the Basic Window, seen in FIGURE 5-2:



FIGURE 5-2: Advanced Button on the Basic Window

5.2 Virtual Servers

In some situations, you might want users on the Internet to be able to access servers on your LAN, such as an FTP Server, Telnet Server or Web Server. Such remote services are accomplished by creating *Virtual Server*.

Each virtual server has its own IP address and shares a single public IP address. It is defined by the Protocol type (*TCP*, *UDP* or *Both*) and a TCP/UDP/Both port number. Only the enabled virtual servers can be accessed by remote users over the Internet.

Note :
Configuring virtual servers may cause filters to be automatically created on the Filters page.

What do you want to do?

- Set up a Client PC on the LAN as a Virtual Server
- Delete Virtual Servers on the LAN

5.2.1. To Set up a Client PC on the LAN as a Virtual Server:

5.2.1.1. On the Advanced navigation bar, click Virtual Servers.

The Virtual Servers page appears with a list of existing virtual servers, seen in FIGURE 5-3:

Service	Public IP Address	Public Port	Private Port	Protocol	Private IP Address
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0

Apply Cancel Help

FIGURE 5-3: Virtual Servers Page

5.2.1.2. If you have enabled DMZ and your Gateway is not configured to retrieve an IP address automatically, select either of the following options from the Choose Interface drop-down list:

- (1) External – Internal: To set up Virtual Server in your LAN network.
- (2) External – DMZ: To set up Virtual Servers in your DMZ network.

5.2.1.3. If you are using the Windows XP operating system, type a remote service name in the Service box.

Note :
It is only available for client PCs using Windows XP. Because Windows XP takes an advantage of the UPnP (Universal Plug and Play) feature of the Company AP Router, it allows client PCs that support UPnP to identify the router automatically.

5.2.1.4. Select a Public IP Address from the drop-down list.

Note :
The IP Address of a DMZ host will not appear in the list.
Type a port number in the Public Port and Private Port boxes, such as 80 for HTTP. For help on which port to choose, refer to Well-known Ports on the right of the page, seen in FIGURE 5-4:

Well-known Ports	
7	Echo
21	FTP
23	TELNET
25	SMTP
53	DNS
79	finger
80	HTTP
110	POP3
113	auth
119	NNTP
161	SNMP
162	SNMP Trap
1723	PPTP

FIGURE 5-4: Well-know Ports

Notes :
Public Port is the TCP/UDP/Both port number used by the server PC on the WAN. It is also called the external port number because this port number is visible to the users on the Internet.
Private Port is the TCP/UDP/Both port number used by the server PC on the LAN. The designated Public Port will be translated into this internal port number

5.2.1.5. Select one of *TCP*, *UDP* and *Both* from the Protocol drop-down list.

5.2.1.6. Type a local IP address of the server PC on the LAN in the Private IP Address box.

5.2.1.7. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.2.2. To Delete Virtual Servers on the LAN:

5.2.2.1. On the Advanced navigation bar, click Virtual Servers.

A list of existing virtual servers appears.

5.2.2.2. For any virtual server you want to delete, select *0.0.0.0* from the Public IP Address drop-down list.

5.2.2.3. Click Apply.

5.3 Filters

On the Filters page, you can set up filters that can selectively allow traffic to pass in and out of your network. The Company AP Router comes with 9 factory default filters for you.

In addition to 9 default filters, some filters may be created automatically to allow Virtual Servers or Special Applications to function.

We strongly recommend that you choose an empty row when you want to set up new filters, because overwriting or deleting these filters may cause some services to be disabled, for example, your client PCs may NOT be able to access the Internet.

Note – If you have overwritten or deleted the factory default filters, you can retrieve them at a later time using the Restore Factory Defaults function on the Tools page. For detailed instructions, see [To Restore the Factory Default Configuration](#).

What do you want to do?

- [Set up a Port Filtering or Raw IP Filter](#)
- [Delete a Port Filtering or Raw IP Filter](#)

5.3.1. To Set up a Port Filtering or Raw IP Filter:

5.3.1.1. On the Advanced navigation bar, click Filters.

The Filters page appears, seen in FIGURE 5-5:

Filtering Page: Page1(1~12) ▾

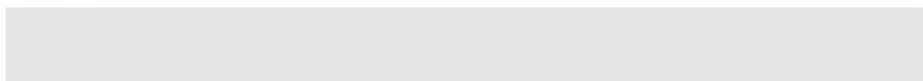
ID	Filtering Layer	Proto Num	Direction	Private Port Range	Protocol
1	Port Filtering ▾	0	Outbound ▾	21 - 21	TCP ▾
2	Port Filtering ▾	0	Outbound ▾	1720 - 1720	TCP ▾
3	Port Filtering ▾	0	Outbound ▾	80 - 80	TCP ▾
4	Port Filtering ▾	0	Outbound ▾	53 - 53	UDP ▾
5	Port Filtering ▾	0	Outbound ▾	25 - 25	TCP ▾
6	Port Filtering ▾	0	Outbound ▾	110 - 110	TCP ▾
7	Port Filtering ▾	0	Outbound ▾	1503 - 1503	TCP ▾
8	Port Filtering ▾	0	Outbound ▾	443 - 443	TCP ▾
9	Raw IP ▾	1	Both ▾	0 - 0	TCP ▾
10	Port Filtering ▾	0	Inbound ▾	8080 - 8080	TCP ▾
11	Port Filtering ▾	0	Inbound ▾	0 - 0	TCP ▾
12	Port Filtering ▾	0	Inbound ▾	0 - 0	TCP ▾

NAT: Enable Disable
 Firewall: Enable Disable
 Remote Management: Enable Disable
 IPSec Pass Through: Enable Disable
 PPTP Pass Through: Enable Disable
 Intrusion Detection: Enable Disable

FIGURE 5-5: Filters Page

5.3.1.2. Select an option from the Filtering Page drop-down list: *1~12, 13~24, 25~36.*

5.3.1.3. If you select Port Filtering from the Filtering Layer drop-down list, do the following action:



5.3.1.3.1. Select a traffic direction from the drop-down list: *Inbound, Outbound and Both.*

5.3.1.3.2. Type the start port number and end port number that you want to allow in the Private Port Range boxes.

5.3.1.3.3. Select a protocol type from the drop-down list: *TCP, UDP and Both.*

5.3.1.4. If you select Raw IP from the Filtering Layer drop-down list, do the following action:

5.3.1.4.1. Type an IP Protocol Number in the Proto Num

Note - It ranges from 0 to 255, but can not be 6 (TCP) or 17 (UDP); otherwise, this port filter will not work.

5.3.1.4.2. Select a traffic direction from the drop-down list: *Inbound Outbound* and *Both*.

5.3.1.4.3. Select an option from the Protocol drop-down list: *TCP, UDP* and *Both*.

5.3.1.5. Optional. Select Enable or Disable for the following additional filtering options:

Parameter	Description
NAT	Allows you to set up NAT (Network Access Translation).
Firewall	Allows you to protect your network with a firewall.
Remote Management	Allows you to access your router's Web-based Administration Tool through your WAN connection.
IPSec Pass Through	Allows you to use IP Security Pass Through.
PPTP Pass Through	Allows you to use PPTP (Point-to-Point Tunneling Protocol), used to enable VPN sessions.
Intrusion Detect	Allows you to detect and record intrusion attempts into your network.

5.3.1.6. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.3.2. To Delete Filters:

You can delete any existing Port Filtering or Raw IP filter, but make sure that you are deleting an unwanted one, otherwise deleting the

filters associated with Virtual Servers or Special Applications may cause to services to collapse down.

5.3.2.1. To Delete a Port Filtering Filter:

5.3.2.1.1. On the Filters page, for any Raw IP filter you want to delete, type *0* in the Private Port Range boxes.

5.3.2.1.2. Click Apply.

5.3.2.2. To Delete a Raw IP Filter:

5.3.2.2.1. On the Filters page, for any Raw IP filter you want to delete, type *0* in the Proto Num box.

5.3.2.2.2. Click Apply.

5.4 IP/URL Block

On the IP/URL Block page, you can create filters that can selectively block users from specific IP addresses and domain names to pass in and out of your network. The Company AP Router provides two ways of blocking users:

- **IP Block:** Allows you to block a single IP address or a range of IP addresses.
- **URL Block:** Allows you to block up to 36 domain names.

Note – This IP/URL Block feature will block in both directions from specified IP addresses or domain names.

What do you want to do?

- **Block a Single IP Address**
- **Block a Range of IP Address**
- **Block a Specific Domain Name**
- **Delete a Specific or All IP Blocks**
- **Delete a Specific or All URL Blocks**

5.4.1. To Block a Single IP Address:

Do either of the following:

5.4.1.1. Click IP/URL Block on the Advanced navigation bar.

5.4.1.2. If you are on the URL Block page, select IP Block on the upper of the page.

The IP Block page appears, seen in FIGURE 5-6:

	IP Block Starting Address	IP Block Ending Address
1	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
2	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
3	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
4	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
5	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
6	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]

Apply Cancel Clear All Help

FIGURE 5-6: IP Block Page

5.4.1.3. In Line 1 – Line 6, type the same IP addresses in both IP Block Starting Address and IP Block Ending Address boxes respectively.

- 5.4.1.4. Optional. You can click Clear All to conveniently delete all the existing IP addresses and then do Step 2.
- 5.4.1.5. When you have completed editing all the IP addresses you want to block, click Apply, or click Cancel to undo your changes.

5.4.2. To Block a Range of IP Address:

- 5.4.2.1. Do either of the following:

Click IP/URL Block on the Advanced navigation bar.
If you are on the URL Block page, select IP Block on the upper of the page.

The IP Block page appears, seen in FIGURE 4-6.

- 5.4.2.2. In Line 1 – Line 6, type the different IP addresses in both IP Block Starting Address and IP Block Ending Address boxes respectively.
- 5.4.2.3. Optional. You can click Clear All to conveniently delete all the existing IP addresses and then do Step 2.
- 5.4.2.4. When you have completed editing all the IP addresses you want to block, click Apply, or click Cancel to undo your changes.

5.4.3. To Block a Specific Domain Name:

- 5.4.3.1. Click IP/URL Block on the advanced navigation bar.

The IP Block page appears, seen in FIGURE 5-6.

- 5.4.3.2. Select URL Block on the IP Block page.

The URL Block page appears, seen in FIGURE 5-7:

URL Block Domain Name	
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>

FIGURE 5-7: URL Block Page

- 5.4.3.3. In Line 1 – Line 36, type the URLs you want to block.

5.4.3.4. Optional. You can click Clear All to conveniently delete all the existing URLs and then do Step 2.

5.4.3.5. When you have completed editing all the domain names you want to block, click Apply, or click Cancel to undo your changes.

5.4.4. To Delete a Specific or All IP Blocks:

5.4.4.1. On the IP Block page, do either of the following:

**For any IP block you want to delete, type 0.0.0.0 in both IP Block Starting Address and IP Block Ending Address boxes respectively.
If you want to delete all IP blocks, click Clear All.**

5.4.4.2. Click Apply.

5.4.5. To Delete a Specific or All URL Blocks:

5.4.5.1. On the URL Block page, do either of the following:

**For any domain name block you want to delete, clear out the URL in the box.
If you want to delete all URL blocks, click Clear All.**

5.4.5.2. Click Apply.

5.5 Special Apps

On the Special Apps page, you can authorize certain ports to communicate with PCs outside your network. It may be necessary for multi-session applications, such as online games and voice conferencing.

There are two ways of set up new special applications on your router:

- **Popular Application Copy:** Allows you to select one of frequently used applications from the Popular Applications drop-down list and copy it to your Special Application Table. Available options are *AIM, Diablo II (1), Diablo II (2), StarCraft, StarCraft III, ICUII, FTP, CUseeMe, MSN Messenger* and *Real Player*.
- **Manual Configuration:** If the application you want to configure is not in the Popular Applications list, you can configure its settings manually.

Before configuring a new special application, would you please check the list of those popular applications first? If it is already in the list, we recommend that you use the Popular Application Copy unless you know exactly which settings to choose.

Notes

Configuring special applications may cause filters to be automatically created on the Filters page.

The Company AP Router provides two factory default special applications for FTP and NetMeeting, if you overwrite them or any other existing application, they will not work.

What do you want to do?

- **[Copy a Popular Application to a Specific Line](#)**
- **[Configure a Special Application Manually](#)**
- **[Delete Special Applications](#)**

5.5.1. To Copy a Popular Application to a Specific Line:

5.5.1.1. On the Advanced navigation bar, click Special Apps.

The Popular Applications list appears on the Special Apps page, seen in FIGURE 5-8:

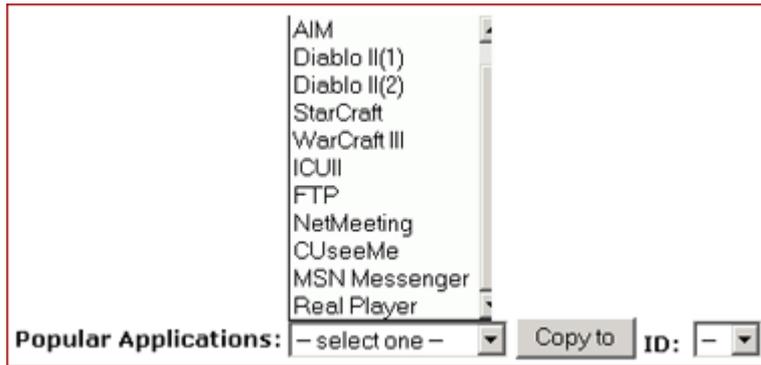


FIGURE 5-8: Popular Applications List

- 5.5.1.2.** Select an option from the Popular Applications drop-down list, including AIM, Diablo II (1), Diablo II (2), StarCraft, StarCraft III, ICUII, FTP, CUseeMe, MSN Messenger and Real Player.

Note :

Make sure the specified ID presents an empty line unless you want to overwrite an existing application.

Select a specific line number from the ID drop-down list.

- 5.5.1.3.** Click Copy to.

- 5.5.1.4.** The selected application's configuration is added to your Special Applications Table on the upper of the page.

- 5.5.1.5.** When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.5.2. To Configure a Special Application Manually:

- 5.5.2.1.** On the Advanced navigation bar, click Special Apps.

- 5.5.2.2.** The Special Apps page appears, seen in FIGURE 5-9:

ID	Protocol	Trigger Port Range	Maximum Activity Interval	Session Chaining	Chaining on UDP	Address Replacement	Address Translation Type	Two Way Only
1	TCP	21 - 21	3000	Disable	Disable	Disable	TCP	Enable
2	TCP	1720 - 1720	30000	Enable	Disable	Enable	TCP	Disable
3	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
4	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
5	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
6	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
7	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
8	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
9	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
10	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
11	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
12	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable

Apply Cancel Help

FIGURE 5-9: Special Apps Page

5.5.2.3. Select a line corresponding to a specific ID.

Note :
Make sure you have selected an empty line unless you want to overwrite an existing application.

Enter the following configuration information:

Parameter	Description
Protocol	Specifies the communication protocol used by the application. <i>Available options are TCP, UDP and Both.</i>
Trigger Port Range	Range of ports used for outgoing traffic. It will trigger the Gateway to accept certain incoming requests.
Maximum Activity Interval	Maximum number of milliseconds after the port trigger function, within which incoming requests will be accepted.
Session Chaining	Allows you to select either Enable or Disable. Specifies whether dynamic sessions can be chained, allowing multi-session triggering.
Chaining on UDP	Allows you to select Enable or Disable only when Session Chaining is enabled. Specifies whether the session chaining is allowed on UDP.

Address Replacement	<p>Allows you to select Enable or Disable only when Chaining on UDP is enabled.</p> <p>Specifies whether binary address replacement should be performed.</p>
Address Translation Type	<p>Allows you to select TCP or UDP only when Address Replacement is enabled.</p> <p>Specifies whether address translation is performed on TCP or UDP packets.</p>
Two Way Only	<p>Allows you to select either Enable or Disable.</p> <p>Specifies that a new session is allowed to be initiated from the same remote host.</p>

5.5.2.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.5.3. To Delete Special Applications:

5.5.3.1. On the Special Apps page, for any application you want to delete, type 0 – 0 in the Trigger Port Range box.

5.5.3.2. Click Apply.

5.6 DMZ Host

On the DMZ Host page, you can expose one or more client PCs in your network to the Internet. It is often used for online games that require unrestricted two-way communications.

The total number of DMZ (Demilitarized Zone) hosts you can have depends on how many Global Addresses you have configured on the Global Address page. For example, if you have defined 5 Global Addresses (including the default IP), you are limited to 5 DMZ hosts. Since the maximum number of Global Addresses is 8, the total number of DMZ hosts you can configure is also 8.

Caution :

Once a PC in your network is designated as DMZ host, it will not have any firewall protection.

What do you want to do?

- Designate a PC in Your Network as a DMZ Host
- Delete DMZ Hosts

5.6.1. To Designate a PC in Your Network as a DMZ Host:

5.6.1.1. On the Advanced navigation bar, click DMZ Host.

The DMZ Host page appears, seen in FIGURE 5-10:

Public IP Address	Private IP Address
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0

Apply Cancel Help

FIGURE 5-10: DMZ Host Page

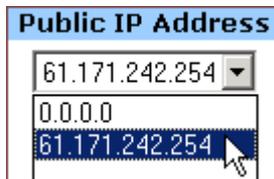
5.6.1.2. Select a Public IP Address from the drop-down list.

5.6.1.3. Type the IP address of a PC in your network that you want to designate as a DMZ Host in the Private IP Address box.

5.6.1.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.6.2. To Delete DMZ Hosts:

5.6.2.1. On the DMZ Host page, for any DMZ host you want to delete, select *0.0.0.0* from the Public IP Address drop-down list.



5.6.2.2. Click Apply.

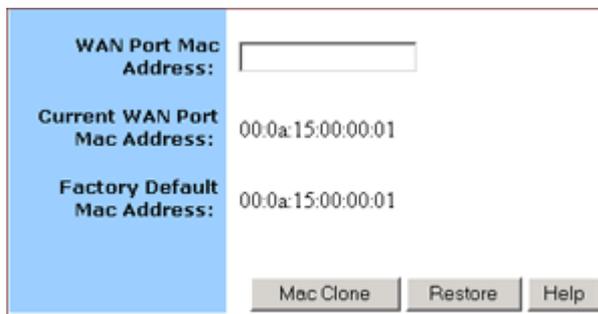
5.7 MAC Clone

If your ISP restricts services at a PC level, using MAC Clone, you can copy a PC MAC (Media Access Control) address to the router. Then what story will begin? The router will appear as a single PC, and multiple PCs in your network will access the Internet via this “*Single PC*”.

5.7.1. To Clone the MAC Address:

5.7.1.1. On the Advanced navigation bar, click MAC Clone.

The MAC Clone page appears with the current WAN port address and the factory default MAC address for your convenience, seen in FIGURE 5-11:



The screenshot shows a web interface for cloning a MAC address. On the left, there is a blue vertical bar containing the labels: "WAN Port Mac Address:", "Current WAN Port Mac Address:", and "Factory Default Mac Address:". To the right of these labels are input fields. The "Current WAN Port Mac Address:" and "Factory Default Mac Address:" fields both contain the value "00:0a:15:00:00:01". The "WAN Port Mac Address:" field is empty. At the bottom of the interface, there are three buttons: "Mac Clone", "Restore", and "Help".

FIGURE 5-11: MAC Clone Page

Note :

You may need to use the Ethernet MAC address of the NIC (Network Interface Card) that your PC is registered with your ISP.

5.7.1.2. Click Mac Clone, or click Restore to retrieve the default settings.

5.8 Dynamic DNS

On the Dynamic DNS page, you can tie up your domain name to a dynamic DNS provider. These providers allow you to associate a static hostname with a dynamic IP address, then you can connect to the Internet with a dynamic IP address and use applications that require a static IP address.

The Company AP Router supports three dynamic DNS providers:

- [DynDNS.org](#)
- [no-IP.com](#)
- [no-IP.com](#)

What do you want to do?

- [Configure a Dynamic DNS Server](#)
- [Disable a Dynamic DNS Server](#)

5.8.1. To Configure a Dynamic DNS Server:

5.8.1.1. On the Advanced navigation bar, click Dynamic DNS.

The Dynamic Server page appears, seen in FIGURE 5-12:



FIGURE 5-12: Dynamic DNS page

5.8.1.2. Select Enable next to Dynamic DNS.

5.8.1.3. Select one of *DynDNS.org*, *no-IP.com*, *no-IP.com* from the Dynamic DNS Provider drop-down list.

5.8.1.4. Type your Domain Name in the box.

5.8.1.5. Type your Account or E-mail in the box.

5.8.1.6. Type your Password or Key in the box.

5.8.1.7. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.8.2. To Disable a Dynamic DNS Server:

5.8.2.1. On the Dynamic DNS page, select Disable next to Dynamic DNS.

5.8.2.2. Click Apply.

5.9 Proxy DNS

On the Proxy DNS page, you can map a domain name to a server IP address. Acting as a DNS server for internal and DMZ networks, it allows you to connect to local machines in your network without using an external DNS server. It simplifies the configuration and management of your network.

What do you want to do?

- [Configure a Proxy DNS Server](#)
- [Delete a Specific or All Proxy DNS Servers](#)
- [Disable the Proxy DNS on Your Router](#)

5.9.1. To Configure a Proxy DNS Server:

5.9.1.1. On the Advanced navigation bar, click Proxy DNS.

The Proxy DNS page appears, seen in FIGURE 5-13:

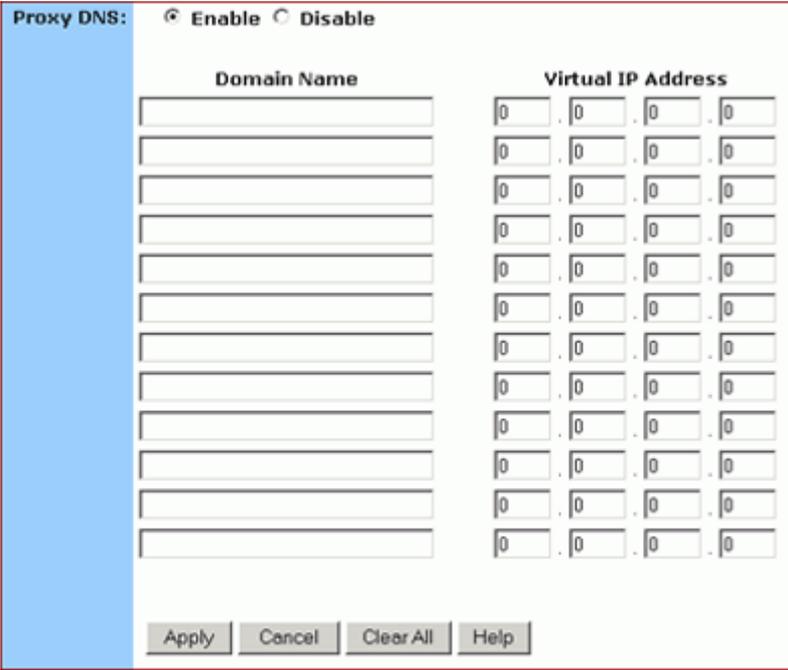


FIGURE 5-13: Proxy DNS Page

5.9.1.2. Select Enable next to Proxy DNS.

5.9.1.3. Type a name for one PC in your network that you want to use as a Proxy DNS server in the Domain Name box.

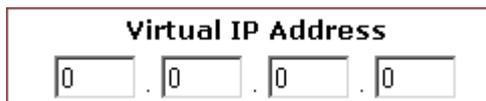
5.9.1.4. Type the IP address for the PC in the Virtual IP Address box.

5.9.1.5. Optional. If you want to delete all the existing Proxy DNS servers first, click Clear All and do Step 3 and Step 4.

5.9.1.6. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.9.2. To Delete a Specific or All Proxy DNS Servers:

5.9.2.1. On the Proxy DNS page, for any Proxy DNS server you want to delete, type *0.0.0.0* in the Virtual IP Address box.



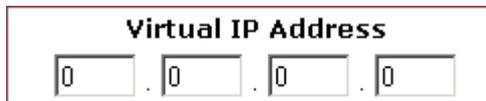
A screenshot of a web form element. It features a rectangular box with a thin red border. At the top center of the box, the text "Virtual IP Address" is displayed in a bold, black font. Below this text, there are four small, square input fields arranged horizontally, separated by dots. Each of these four input fields contains the digit "0", representing the IP address "0.0.0.0".

5.9.2.2. If you want to delete all the existing Proxy DNS servers, click Clear All.

5.9.2.3. Click Apply.

5.9.3. To Disable the Proxy DNS on Your Router:

5.9.3.1. On the Proxy DNS page, for any Proxy DNS server you want to delete, type *0.0.0.0* in the Virtual IP Address box.



A screenshot of a web form element, identical to the one in section 5.9.2. It features a rectangular box with a thin red border. At the top center of the box, the text "Virtual IP Address" is displayed in a bold, black font. Below this text, there are four small, square input fields arranged horizontally, separated by dots. Each of these four input fields contains the digit "0", representing the IP address "0.0.0.0".

5.9.3.2. If you want to delete all the existing Proxy DNS servers, click Clear All.

5.9.3.3. Click Apply.

5.10 SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of TCP/IP (Transmission Control protocol/Internet Protocol) suite and enables you to control and monitor the network in a simple way.

On the SNMP page, you can edit the basic Agent information and also configure up to 6 SNMP trap receiver's IP Addresses. When a trap condition occurs, your router will send an SNMP trap message to any NMS (Network Management System) specified as trap receivers, for example, when power supply errors occur.

Notes :

NMS (Network Management System) is an SNMP management application together with the computer it runs on.

Currently the Company AP Router supports SNMPv1 (SNMP version 1) and SNMPv2 (SNMP version 2) which have a number of features in common except for some enhancements.

And moreover, you can specify different community names for authenticating access to the management information, which function as embedded passwords:

- **Read:** Gives you READ access to all the management information, but does not allow WRITE access.
- **Write:** Gives you both READ and WRITE access to all the management information.

Note :

The community name definitions on your NMS must match at least one of the above two community name definitions.

What do you want to do?

- **Configure Agent Information, SNMP Trap Host IP Addresses and Community Names on Your Router**
- **Delete an Existing SNMP Trap Receiver**
- **Delete SNMP Community Names**

5.10.1. To Configure Agent Information, SNMP Trap Host IP Addresses and Community Names on Your Router:

5.10.1.1. On the Advanced navigation bar, click SNMP.

The SNMP page appears, seen in FIGURE 5-14:

The screenshot shows the SNMP configuration interface. The left sidebar is blue. The main content area has a white background. At the top, there are three text input fields: 'Name' (containing 'SOHO Router'), 'Contact', and 'Location'. Below these are six rows of IP address input fields, labeled 'SNMP Trap Host IP 1' through 'SNMP Trap Host IP 6'. Each row has four small input boxes separated by dots. At the bottom of the main area are three buttons: 'Apply', 'Cancel', and 'Help'. Below the main area is a 'Community List' section. It has a table with three columns: 'SNMP Community', 'SNMP Access', and an action column. The table has one row with ID '1', Name 'None', and Access 'None'. There are '<< Add' and 'Delete' buttons next to the table.

FIGURE 5-14: SNMP Page

Enter the following Agent information:

Parameter	Description
Name	<p>Specifies an administratively-assigned name for this managed node, like <i>SOHO Router</i>.</p> <p>It is a string of the maximum 31 alphanumeric characters.</p>
Contact	<p>Specifies the contact person of this managed node, plus phone number, Email address, etc.</p> <p>It is a string of the maximum of 255 alphanumeric characters.</p>
Location	<p>Specifies the physical location of this managed node, for example, city, address and specific office location.</p> <p>It is a string of the maximum of 255 alphanumeric characters.</p>

5.10.1.2. To send SNMP trap messages to any NMS, type up to 6 trap receiver IP addresses in the SNMP Trap Host IP Address 1 – SNMP Trap Host IP Address 6 boxes.

5.10.1.3. To secure SNMP with community names, do the following action:



5.10.1.3.1. Type a string in the SNMP Community box, like Public.

5.10.1.3.2. Select an option from the SNMP Access drop-down list, for example, Read.

Note :

Usually, we define a string of “*Public*” for Read access and “*Private*” for Read-Write access.

5.10.1.3.3. Click Add. If you want to add more community names, do Step 4.1 – Step 4.3 again.

5.10.1.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

5.10.2. To Delete an Existing SNMP Trap Receiver:

5.10.2.1. On the SNMP page, for any SNMP trap receiver that you want to delete, enter *0.0.0.0* in the SNMP Trap Host IP Address box.

Community List:			
	SNMP Community	SNMP Access	
	<input type="text"/>	Read	<< Add
1	Public	Read	Delete

5.10.2.2. Click Apply.

5.10.3. To Delete SNMP Community Names:

5.10.3.1. On the SNMP page, for any SNMP community name that you want to delete, click Delete in the corresponding row.

5.10.3.2. Click Apply.

5.11.1.2. Enter the following static route information:

Parameter	Description
Destination LAN IP	Specifies the network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of this Destination LAN IP, the 4th field can be left at 0.
Subnet Mask	Specifies the Subnet Mask used on the remote LAN segment. For class "C" networks, the standard Network Mask is 255.255.255.0.
Gateway	Specifies the IP Address of the router on the local LAN segment to which this device is attached. Note that it is NOT the router on the remote LAN segment.
Hop	Specifies the number of routers that must be traversed to reach the remote LAN segment. Valid values are 1 to 16.
Interface	Specifies the interface through which the router goes to the next hop or a particular network. Available options are WAN, LAN and DMZ.

5.11.1.3. Click <<Add.

The new static route appears in the static routing list.

5.11.2. To Delete a Static Route:

5.11.2.1. On the Static Routing page, for any static route that you want to delete, review the relevant information, seen in FIGURE 5 – 15.

5.11.2.2. Click Delete.

6. Glossary

IEEE 802.11 Standard

The IEEE 802.11 Wireless LAN standards subcommittee, which is formulating a standard for the industry.

Access point

An Internet working device that seamlessly connects wired and wireless networks together.

Ad hoc

An ad hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

BSSID

A specific ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSSID.

DHCP

Dynamic Host Configuration Protocol - a method in which IP addresses are assigned by a server dynamically to clients on the network. DHCP is used for dynamic IP addressing and requires a dedicated DHCP server on the network.

DSSS

Direct Sequence Spread Spectrum. This is the method the wireless adapters use to transmit data over the frequency spectrum. An alternative method is frequency hopping. Direct sequence spreads the data over one frequency range (channel) while frequency hopping jumps from one narrow frequency band to another many times per second.

ESSID

An infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an extended service set (ESS). Users within an ESS can roam freely between BSSs while served as a continuous connection to the network wireless stations and access points within an ESS must be configured with the same ESSID and the same radio channel.

Ethernet

Ethernet is a 10/100Mbps network that runs over dedicated home/office wiring. Users must be wired to the network at all times to gain access.

Gateway

A gateway is a hardware and software device that connects two dissimilar systems, such as a LAN and a mainframe. In Internet terminology, a gateway is another name for a router. Generally a gateway is used as a funnel for all traffic to the Internet.

IEEE

Institute of Electrical and Electronics Engineers

Infrastructure

An integrated wireless and wired LAN is called an infrastructure configuration. Infrastructure is applicable on an enterprise scale for wireless access to a central database, or wireless application for mobile workers.

ISM Band

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the so-called ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe.

LAN

Local Area Network. A LAN is a group of computers, each equipped with the appropriate network adapter connected by cable/air that share applications, data, and peripherals. All connections are made via cable or wireless media, but a LAN does not use telephone services. It typically spans a single building or campus.

Network

A network is a system of computers that is connected. Data, files, and messages can be transmitted over this network. Networks may be local or wide area networks.

Protocol

A protocol is a standardized set of rules that specify how a communication is to take place, including the format, timing, sequencing and/ or error checking.

SSID

Service Set Identifier. A network ID unique to a network. Only clients and access points that share the same SSID are able to communicate with each other. This string is case-sensitive.

SNMP

Simple Network Management Protocol is the network management protocol of TCP/IP. In SNMP, agents-which can be hardware as well as software-monitor the activity in the various devices on the network and report to the network console workstation. Control information about each device is maintained in a structure known as a management information block.

Static IP addressing

A method of assigning IP addresses to clients on the network. In networks with static IP address, the network administrator manually assigns an IP address to each computer. Once a static IP address is assigned, a computer uses the same IP address every time it reboots and logs on to the network, unless it is manually changed.

TCP/IP

Transmission Control Protocol / Internet Protocol. TCP/IP is the protocol suite developed by the Advanced Research Projects Agency (ARPA). TCP governs how a packet is sequenced for transmission the network. The term "TCP/IP" is often used generically to refer to the entire suite of related protocols.

Transmit / Receive

The wireless throughput in bytes per second (Bps) averaged over two seconds.

WAN

Wide Area Network. A WAN consists of multiple LANs that are tied together via telephone services and / or fiber optic cabling. WANs may span a city, a state, a country, or even the world.

acer
we hear you

<http://www.acer-euro.com>

Acer

WLAN 11g Breitband Router

Benutzerhandbuch



This product is in compliance with the essential requirements and other relevant provisions of the

R&TTE directive 1999/5/EC.



Product Name: Acer WLAN 11g Broadband Router

Model Name : WLAN-G-RU2

COUNTRY		CHANNELS	MAX. OUT POWER	
			INDOOR	OUTDOOR
Spain	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
France	2400-2454 MHz	1-8	< 100 mW EIRP	< 100 mW EIRP
France	2454-2483.5 MHz	9-13	< 100 mW EIRP	< 10 mW EIRP
Italy	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
UK	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Netherlands	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Germany	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Austria	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Belgium	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Switzerland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Luxemburg	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Ireland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Portugal	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Norway	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Denmark	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Finland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Iceland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Greece	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Lichtenstein	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Sweden	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP

Copyright

Copyright © 2004 Acer Inc. Alle Rechte vorbehalten. Dieses Handbuch darf weder reproduziert, weitergegeben, kopiert, in einem Dokumentenverwaltungssystem gespeichert, in eine andere Sprache oder eine andere Computersprache übersetzt werden, noch in irgendeiner Form, sei es elektronisch, mechanisch, magnetisch, optisch, chemisch, oder sonstwie ohne schriftliche Genehmigung von Acer Inc. vervielfältigt oder verwendet werden.

Verzichteleistung

Die Firma lehnt jegliche Gewährleistung, sei sie explizite oder implizite, bezüglich des Inhalts dieser Anleitung, und insbesondere jegliche Garantie bezüglich einer Handelsüblichkeit oder Eignung für einen bestimmten Zweck ab. Alle in dieser Anleitung beschriebene Software wird, „wie sie vorliegt“ verkauft oder lizenziert. Sollten sich die Programme nach dem Kauf als fehlerhaft erweisen, so übernimmt der Käufer (und nicht diese Firma, ihr Vertrieb oder ihr Händler) die vollständigen Kosten sämtlicher anfallenden Reparaturen und Serviceleistungen, sowie für jegliche daneben entstandenen Schäden oder Folgeschäden, die sich aus einem Fehler dieser Software ergeben haben. Desweiteren behält sich Acer Inc. das Recht vor, dieses Handbuch zu überarbeiten und den Inhalt von Zeit zu Zeit zu ändern, ohne sich zur Bekanntgabe solcher Überarbeitungen oder Änderungen zu verpflichten.

Technischer Support :

Bei technischen Fragen zu unseren Produkten, wenden Sie sich bitte an Ihren Fachhändler oder an unsere PremiumLine. In Deutschland erreichen Sie diesen Support von Montags – Freitags 09:00 – 18:00 Uhr unter:

01907 / 88 788 1,22 €/min (Nur für Deutschland)

Treiber und Updates erhalten Sie unter: <http://www.acer.de>

Inhalt

1. ÜBERSICHT	2
1.1 Produkteigenschaften	2
1.2 Systemanforderungen	2
1.3 Anwendungen	2
2. Installation Ihres Routers.....	3
2.1 Installationsanweisungen	3
3. Vorbereitung Ihres Netzwerks	4
3.1 Konfigurieren von Windows für IP-Netzwerke	4
3.2 Konfigurieren von Windows, um eine dynamische IP-Adresse zu erhalten:	4
3.3 Beschaffen von ISP-Informationen	6
4. Grundlegende Funktionen	7
4.1 Zum Öffnen des Web-basierten Administrations-Tools:	7
4.2 Setup	9
4.3 Global Address	13
4.4. Wireless	17
4.5 Tools	26
4.6 Status	31
4.7 DHCP	34
4.8 Log	37
4.9 Statistiken	41
5. Erweiterte Funktion	43
5.1. Umschalten zwischen Grundfunktionen und erweiterten Funktionen:	43
5.2 Virtuelle Server	44
5.3 Filter	48
5.4 IP/URL Block	52
5.5 Spezielle Anwendungen	56
5.6 DMZ Host	60
5.7 MAC Clone	62
5.8 Dynamic DNS	63
5.9 Proxy DNS	65
5.10 SNMP	67
5.11 Statisches Routing	71
6. Glossar.....	73

1. ÜBERSICHT

1.1 Produkteigenschaften

- Kompatibel mit den Standards IEEE 802.11g und 802.11b
- Hocheffizientes Design für unschlagbare Performance
- Große Netzwerksicherheit durch WEP- und 802.1X-Verschlüsselung
- Datenübertragungsraten bis zu 54 Mbps bei 802.11g und 11 Mbps bei 802.11b mit großer Reichweite; eine Übertragungsrate von bis zu 54 Mbps bei 802.11g für Rohdaten
- Schnelles und einfaches Einrichten mit Web-basierter Management Utility

1.2 Systemanforderungen

- Betriebssysteme Windows 98, 98SE, Millennium Edition (ME), 2000 und XP
- Microsoft Internet Explorer 5.5 oder höher
- Breitband-Verbindung zum Internet mit DSL- oder Kabelmodem und Internetzugang
- PC mit 10 Mbps oder 10/100 Mbps Ethernet-Anschluss für Unterstützung von TCP/IP-Protokoll
- Ein CD-ROM-Laufwerk

1.3 Anwendungen

- Heim- und SOHO-Netzwerke zur gemeinsamen Nutzung von Geräten und Wireless-Multimedia
- Ein Wireless-Büro bietet größere Reichweite für Heim- und SOHO-Ethernet
- Ermöglicht drahtlose Datenübertragung zwischen verschiedenen Gebäuden
- Eingebauter Infrastruktur-Modus
- Der Router ist die ideale Lösung für:

Vorübergehend eingerichtete LANs wie zum Beispiel bei Handelsausstellungen und Sitzungen

Ermöglicht Anpassung von LANs an häufig wechselnde Umgebungen

Ermöglicht Fernzugriff auf Informationen im Firmennetzwerk, zum Beispiel E-Mails oder die Firmenhomepage

2. Installation Ihres Routers

In diesem Kapitel erfahren Sie, wie Sie Ihren Router anschließen.

2.1 Installationsanweisungen

Zum Anschließen des Routers:

- 2.1.1.** Stellen Sie sicher, dass alle Geräte abgeschaltet sind, einschließlich Router, Desktop- oder Laptop-PCs, Kabel- und DSL-Modem, etc.
- 2.1.2.** Schließen Sie den WAN-Anschluss des Routers an das Kabel- und das DSL-Modem, den Ethernet-Server oder den Hub an.
- 2.1.3.** Schließen Sie Ihre Client-PCs an die LAN-Anschlüsse an.
- 2.1.4.** Verbinden Sie das Netzteil (5 V DC, 1,2 A) mit der Anschlussbuchse des Routers und schließen Sie das Stromkabel am Hauptausgang an.
- 2.1.5.** Schalten Sie Ihre PCs ein.

3. Vorbereitung Ihres Netzwerks

In diesem Kapitel erfahren Sie, was vor dem Konfigurieren Ihres Netzwerks zu tun ist.

Bevor Sie Ihren Router konfigurieren, müssen Sie die Computer in Ihrem Netzwerk für ein TCP/IP-Netzwerk einrichten und ggf. die relevanten ISP-Informationen einholen.

3.1 Konfigurieren von Windows für IP-Netzwerke

Jeder Computer in Ihrem Netzwerk sollte für die TCP/IP-Netzwerkanbindung konfiguriert werden. Es gibt zwei Wege, Ihre Computer zu konfigurieren:

- Es wird empfohlen, DHCP zu verwenden, da hier einfach gewählt werden kann, eine IP-Adresse automatisch zu erhalten. Zu detaillierten Anweisungen siehe [Konfigurieren von Windows, um eine dynamische IP-Adresse zu erhalten](#)
- Wenn Sie DHCP nicht verwenden, müssen Sie jedem Computer manuell eine IP-Adresse zuweisen. Zu detaillierten Anweisungen beachten Sie bitte Ihre Windows-Dokumentation.

3.2 Konfigurieren von Windows, um eine dynamische IP-Adresse zu erhalten:

3.2.1. Klicken Sie auf Start, wählen Sie dann Einstellungen > Netzwerk und DFÜ-Verbindung.

3.2.2. Wählen Sie den Namen Ihrer ISP-Verbindung.

Das Dialogfeld 'Local Area Connection Status' erscheint, siehe **Abbildung 3-1:**

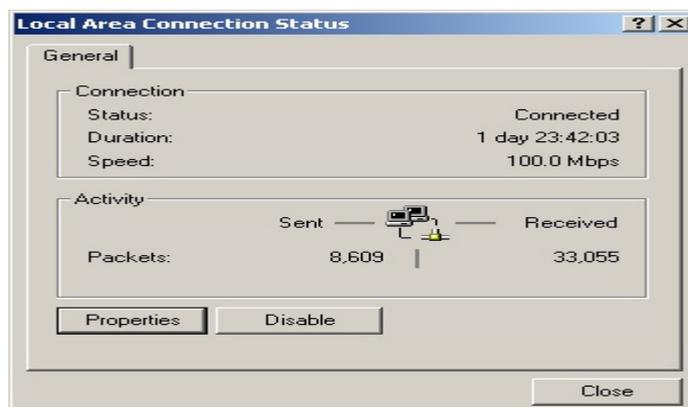


ABBILDUNG 3-1: Das Dialogfeld 'Local Area Connection Status'

3.2.3. Klicken Sie auf 'Properties'.

Das Dialogfeld 'Local Area Connection Properties' erscheint wie in ABBILDUNG 3-2 dargestellt:

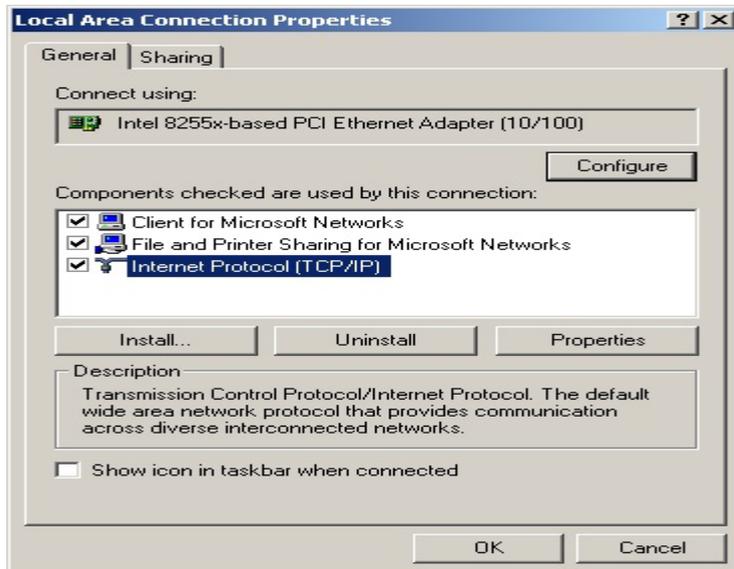


ABBILDUNG 3-2: Das Dialogfeld 'Local Area Connection Eigenschaften'.

3.2.4. Klicken Sie zuerst auf 'Internet Protocol (TCP/IP)', dann auf 'Properties'.

Das Dialogfeld 'Internet Protocol (TCP/IP) Properties' erscheint wie in ABBILDUNG 3-3 dargestellt:

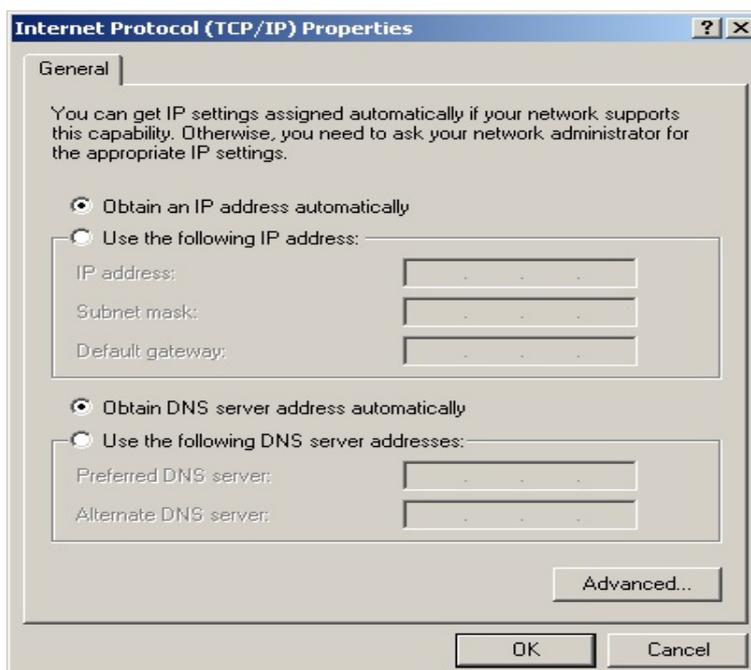


ABBILDUNG 3-3: Das Dialogfeld 'Internet Protocol (TCP/IP) Properties'

3.2.5. Klicken Sie auf 'Obtain an IP address automatically' und 'Obtain DNS server address automatically'.

3.2.6. Klicken Sie auf 'OK'.

Sie müssen Ihren Computer jetzt oder später neu starten.

Hinweis :

Die oben genannten Verfahrensschritte gelten nur für Windows 2000. Für Window 95/98/ME/NT/XP beachten Sie bitte Ihre Windows-Dokumentation.

3.3 Beschaffen von ISP-Informationen

Sie müssen die relevanten Informationen Ihres ISP erfragen, bevor Sie Ihren Router konfigurieren, zum Beispiel:

- **Hat Ihr ISP Ihnen eine statische oder dynamische IP-Adresse zugewiesen? Wenn Sie eine statische IP-Adresse erhalten haben, wie lautet sie?**
- **Verwendet Ihr ISP PPPoE? Wenn ja, was ist Ihr PPPoE-Benutzername und -Passwort?**

Wenn Sie nicht hierüber nicht sicher sind, wenden Sie sich an Ihren ISP.

4. Grundlegende Funktionen

In diesem Kapitel erfahren Sie, wie die Grundfunktionen, die der Unternehmens-AP-Router bereitstellt, einschließlich Setup, Global Address, Wireless Tools, Status, DHCP, Log und Drucker verwendet werden.

Der Acer WLAN 11g Breitband-Router bietet Ihnen ein Web-basiertes Administrations-Tool, mit dem Sie den Router leicht einrichten und die Grundeinstellungen Ihren Anforderungen entsprechend vornehmen können. Sie können dieses Web-basierte Tool aus jedem Computer ihres Netzwerks verwenden.

Hinweise:

Für die Verwendung dieses Web-basierten Tools wird der Microsoft Internet Explorer 5.0 oder neuer besonders empfohlen. Die Beispielabbildungen in diesem Kapitel dienen nur der Erläuterung. Sie können von Ihren Router-Bildschirmen geringfügig abweichen.

4.1 Zum Öffnen des Web-basierten Administrations-Tools:

4.1.1. Öffnen Sie den Browser auf Ihrem PC.

4.1.2. Geben Sie *http://192.168.62.1* in die Adresszeile ein.

Das Dialogfeld zur Anmeldung erscheint wie in ABBILDUNG 4-1 dargestellt:



ABBILDUNG 4-1: Das Dialogfeld zur Anmeldung

4.1.3. Tippen Sie in das Feld 'User Name' *admin* ein.

4.1.4. Geben Sie das Passwort in das entsprechende Feld ein.

Hinweis :

Das voreingestellte Passwort ist “1234”. Sie können das Passwort unter dem Menüpunkt 'Tools' ändern. Zu detaillierten Anweisungen siehe Das Administrator-Passwort für Ihren Router ändern.

4.1.5. Optional: Wählen Sie das Kontrollkästchen 'Save this password in your password list', um das Passwort dauerhaft im Administrations-Tool zu speichern.

4.1.6. Klicken Sie auf 'OK'.

Das Unternehmens-AP-Router-Administrations-Tool erscheint.

Hinweis :

Wenn das Netzwerk eine Zeit inaktiv war, meldet Sie das Administrations-Tool ab; der Router wird Sie in diesem Fall auffordern, sich erneut anzumelden.

4.2 Setup

Die Setup-Seite ermöglicht Ihnen, die Parameter der Grundkonfiguration für Ihren Router, wie z.B. *Host Name*, *Domain Name*, *LAN IP Address*, *WAN IP Address*, *PPPoE Login*, *UPNP*, etc. zu bearbeiten.

In den meisten Fällen sind die Voreinstellungen für Ihre Zwecke ausreichend. Dennoch können unterschiedliche ISPs (Internet Service Provider) bestimmte Anforderungen haben; wenden Sie sich im Zweifelsfall an Ihren ISP.

4.2.1. Konfiguration der Setup-Parameter:

4.2.1.1. Klicken Sie in der Navigationsleiste auf 'Setup'.

Die Setup-Seite wird angezeigt wie in ABBILDUNG 4-2 dargestellt:

The screenshot displays the 'Setup' page of a router's web interface. The page is organized into sections on the left and right. The left sidebar contains labels for various configuration items: Host Name, Domain Name, Firmware Version, Time, Set Time Zone, Daylight Savings, Daylight Period, LAN IP Address, WAN IP Address, PPPoE Login, and UPNP. The right side contains the corresponding input fields and options. Host Name and Domain Name are empty text boxes with a note '(Required by some ISPs)'. Firmware Version shows '20-06-07, Oct 20 2003 17:09:22'. Time is 'Thu Nov 6 3:52:57 2003'. Set Time Zone is a dropdown menu set to '(GMT-08:00) Pacific Time (US&Canada): Tijuana'. Daylight Savings has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. Daylight Period shows 'JAN' and '01' for both start and end dates. LAN IP Address has 'Device IP Address' (192.168.62.1) and 'Subnet Mask' (255.255.255.0). WAN IP Address has radio buttons for 'Obtain an IP Address Automatically' (selected) and 'Specify an IP Address'. The 'Specify an IP Address' section includes fields for WAN IP Address, Subnet Mask, ISP Gateway Address, and three DNS servers (all set to 0.0.0.0). PPPoE Login has radio buttons for 'Enable' and 'Disable', with 'Enable' selected. It includes fields for 'User Name' (ad50159026) and 'Password' (masked with asterisks). There are radio buttons for 'Connect on Demand' and 'Connect Manually' (selected), and a checked checkbox for 'Max Idle Time' set to 10 minutes. UPNP has radio buttons for 'Enable' and 'Disable', with 'Enable' selected. At the bottom are 'Apply', 'Cancel', and 'Help' buttons.

ABBILDUNG 4-2: Die Setup-Seite

- 4.2.1.2. Geben Sie Host-Namen, System-Namen oder Account-Namen in das Feld 'Host Name' ein, wenn Ihr ISP dies erfordert.
- 4.2.1.3. Geben Sie den Domain-Namen Ihres ISP in das Feld ein, wenn Ihr ISP dies erfordert, z.B. *xyz.isp.com*.
- 4.2.1.4. Optional: Überprüfen Sie die Nummer der Firmware Version und die Datumsinformation Ihrer Version.
- 4.2.1.5. Wählen Sie eine Zeitzone aus dem Dropdown-Menü 'Set Time Zone', z.B. *(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi*.
- 4.2.1.6. Wenn die Zeit auf Sommerzeit umgestellt werden soll, klicken Sie unter 'Daylight Savings' auf 'Enable' und wählen Sie Start- und Enddatum der Sommerzeit aus dem Dropdown-Menü.
- 4.2.1.7. Wenn Sie die Sommerzeit nicht verwenden möchten, klicken Sie auf 'Disable'. Wenn Sie unter 'Daylight Savings' 'Disable' gewählt haben, werden die Angaben unter 'Daylight Period' nicht berücksichtigt.
- 4.2.1.8. Optional: Überprüfen Sie die Geräte-IP-Adresse und die Subnet Mask neben 'LAN IP Address' und ändern Sie die Informationen falls nötig.

LAN IP Address:	Device IP Address:	<input type="text" value="192"/>	.	<input type="text" value="168"/>	.	<input type="text" value="62"/>	.	<input type="text" value="1"/>
	Subnet Mask:	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="0"/>

Hinweise:

***Device IP Address* und *Subnet Mask* sind nur für Nutzer im LAN (Local Area Network) unsichtbar.**

In den meisten Fällen müssen Sie keine Änderungen an der LAN IP-Adresse vornehmen. Wenn Sie die LAN-IP-Adresse ändern, wenn DHCP aktiviert ist, müssen Sie Ihre Client-PCs neu starten; Andernfalls müssen Sie die IP-Adressen Ihres Clients manuell neu konfigurieren.

- 4.2.1.9. Wenn Sie auf der DHCP-Seite die Funktion DMZ aktiviert haben, überprüfen Sie die DMZ-IP-Adresse und die Subnet-Adresse neben 'DMZ IP Address' und ändern Sie die Informationen, falls nötig.
- 4.2.1.10. Für WAN IP-Adressen (Wide Area Network, auch Public IP genannt) wählen Sie entweder 'Obtain an IP Address automatically' oder, wenn Ihr ISP Ihnen eine statische IP-Adresse zugewiesen hat, 'Specify an IP Address'.

Hinweis:

Wenn Sie 'Obtain an IP Address' automatisch gewählt haben, überspringen Sie Schritt 11.

4.2.1.11. Optional: Wenn Sie 'Specify an IP Address' wählen, geben Sie die 'WAN IP Address', 'Subnet Mask', 'ISP Gateway Address' und den 'DNS' in die Felder ein, wie in ABBILDUNG 4-3 gezeigt. Sie erhalten diese Informationen von Ihrem ISP.

Specify an IP Address

WAN IP Address: [0] . [0] . [0] . [0]

Subnet Mask: [0] . [0] . [0] . [0]

ISP Gateway Address: [0] . [0] . [0] . [0]

DNS

1: [0] . [0] . [0] . [0]

2: [0] . [0] . [0] . [0]

3: [0] . [0] . [0] . [0]

ABBILDUNG 4-3: WAN IP Address - Specify an IP Address

4.2.1.12. Wenn Ihr ISP PPPoE (Point to Point Protocol over Ethernet) verwendet, klicken Sie neben 'PPPoE Login' auf 'Enable'; Sonst klicken Sie auf 'Disable'. Zu detaillierten Anweisungen zur Einstellung der PPPoE Login-Parameter in ABBILDUNG 3-4, siehe Einstellen der PPPoE Login-Parameter unten.

Hinweise:

Wenn Sie PPPoE verwenden, kann Ihr ISP Sie aus Sicherheitsgründen dazu auffordern, sich mit User-Name und Passwort zu identifizieren.

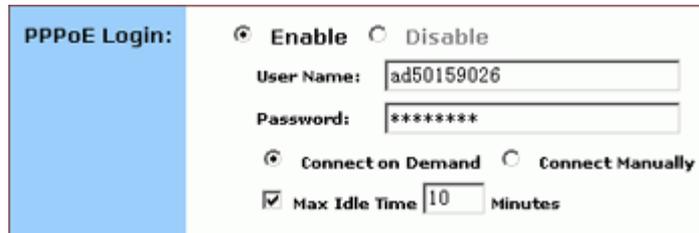
Wenn Sie PPPoE aktivieren, stellen Sie sicher, dass Sie alle vorhandenen Anwendungen auf jedem Computer in Ihrem Netzwerk deinstallieren.

4.2.1.13. Wenn Sie UPNP (Universal Plug and Play) verwenden möchten, um Geräte wie PCs, Router und andere an ein Netzwerk anzuschließen, und die Geräte sich gegenseitig automatisch erkennen sollen, klicken Sie neben 'UPNP' auf 'Enable'; Sonst klicken Sie auf 'Disable'.

4.2.1.14. Wenn Sie Ihre Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

4.2.2. Einstellen der PPPoE Login-Parameter:

4.2.2.1. Klicken Sie neben 'PPPoE Login' auf 'Enable'.



PPPoE Login: Enable Disable

User Name:

Password:

Connect on Demand Connect Manually

Max Idle Time Minutes

ABBILDUNG 4-4: Einstellen der PPPoE Login-Parameter

4.2.2.2. Geben Sie User Name und Password, die Sie von Ihrem ISP erhalten, ein.

4.2.2.3. Sie können zwischen den Verbindungstypen 'Connect on Demand' oder 'Connect Manually' wählen.

4.2.2.4. Optional: Wenn Sie die Dauer der Netzwerkinaktivität begrenzen möchten, wählen Sie 'Max Idle Time' und geben Sie die maximale Dauer in Minuten ein.

4.3 Global Address

Auf der Seite 'Global Address' können Sie die NAT (Network Address Translation) einstellen, um

Hinweise:

Wenn Sie die Global Address-Zuordnung verwenden möchten, müssen Sie NAT auf der Seite 'Filters' aktivieren. Zu detaillierten Anweisungen siehe Einrichten eines Port-Filters oder Raw-IP-Filters.

Wenn Sie sich für die automatische Zuweisung einer IP-Adresse entschieden haben, müssen Sie diese Funktion nicht verwenden. Stattdessen wird die voreingestellte, öffentliche IP-Adresse auf der Seite 'Global Address' angezeigt.

Internal-to-external-IP-Adressen bereitzustellen.

Haben Sie DMZ auf der DHCP-Seite aktiviert? Je nachdem, ob DMZ aktiviert ist, können Sie verschiedene Verfahren befolgen.

Was möchten Sie tun?

- Einstellen der Global Address mit deaktiviertem DMZ
- Einstellen der Global Address mit aktiviertem DMZ
- Entfernen Globaler Adressen

4.3.1. Einstellen der Global Address mit deaktiviertem DMZ:

4.3.1.1. Klicken Sie in der Navigationsleiste auf 'Global Address'.

Die Seite 'Global Address' mit deaktiviertem DMZ wird angezeigt wie in ABBILDUNG 4-5 dargestellt:

Setup	Global Address	Wireless	Tools	Status	DI/ICP	Log	Statistics
1: 0.0.0.0 (default gateway)							
2: <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/>							
3: <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/>							
4: <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/>							
5: <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/>							
6: <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/>							
7: <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/>							
8: <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>							

ABBILDUNG 4-5: Global Address mit deaktiviertem DMZ

4.3.1.2. Beachten Sie die erste Zeile in der Abbildung oben. Sie zeigt die voreingestellte WAN-IP-Adresse, die auf der Setup-Seite angegeben ist. Wenn Ihr ISP Ihnen automatisch eine IP-Adresse zuweist, wird sie hier angezeigt.

4.3.1.3. In Zeile 2 – Zeile 8 können Sie bis zu 7 zusätzliche, statische, externe IP-Adressen angeben, die Ihnen von Ihrem ISP zugewiesen werden.

4.3.1.4. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

4.3.2. Einstellen der Global Address mit aktiviertem DMZ:

4.3.2.1. Klicken Sie in der Navigationsleiste auf 'Global Address'.

Die Seite 'Global Address' mit aktiviertem DMZ wird angezeigt wie in ABBILDUNG 4-6 dargestellt:

Setup	Global Address	Wireless	Tools	Status	DHCP	Log	Statistics
External-Internal							
1	<input type="text" value="200"/>	<input type="text" value="168"/>	<input type="text" value="76"/>	<input type="text" value="2"/>			
2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
4	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
5	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
6	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
External-DMZ							
1	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
4	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
5	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
6	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>			
				<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>	<input type="button" value="Help"/>	

ABBILDUNG 4-6: Global Address mit aktiviertem DMZ

- 4.3.2.2.** Beachten Sie die erste Zeile in der Abbildung oben. Sie zeigt die voreingestellte WAN-IP-Adresse, die auf der Setup-Seite angegeben ist. Wenn Ihr ISP Ihnen automatisch eine IP-Adresse zuweist, wird sie hier angezeigt.
- 4.3.2.3.** Neben External - Internal können Sie bis zu 6 zusätzliche, statische, externe IP-Adressen angeben, die Ihnen von Ihrem ISP zugewiesen werden.
- 4.3.2.4.** Neben External – DMZ definieren Sie für Ihr DMZ-Netzwerk bis zu 6 statische, externe globale IP-Adressen, die Ihnen von Ihrem ISP zugewiesen werden.
- 4.3.2.5.** Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

4.3.3. Entfernen Globaler Adressen:

4.3.3.1. Klicken Sie in der Navigationsleiste auf 'Global Address'.

4.3.3.2. Wenn Sie einen Eintrag löschen möchten, geben Sie *0.0.0.0* ein und klicken Sie auf 'Apply'.

4.4. Wireless

Mit der Einstellung 'Wireless' können Sie Ihren Router für den drahtlosen Zugriff konfigurieren. Die Wireless-Seite besteht aus drei Teilen:

- **'Radio Settings'**: Ermöglicht Ihnen, Ihr Gateway für Wireless Access zu konfigurieren, einschließlich *Wireless Enable/Disable, Mode, ESSID, Beacon Interval, RTS Threshold, Preamble Type, Distribution System, etc.*
- **'Security Setting'**: Ermöglicht Ihnen, die Sicherheitseinstellungen Ihres Gateway zu konfigurieren.
- **'Status'**: Ermöglicht Ihnen, die AP-Funk-Statistiken Ihres Gateways und Wireless-Geräte, die der AP (Access Point) erkannt hat, anzuzeigen.

Sie können auf der Wireless-Seite zwischen diesen drei Teilen einfach hin und her schalten.

Auf der Seite 'Radio Settings' wurde das Wireless Distribution System gemäß IEEE 802.11-Standard auf dem Unternehmens-AP-Router verfügbar gemacht. Daher ist es möglich, Access Points drahtlos unter Verwendung von bis zu 8 MAC-Adressen von PC-Karten anzuschließen, so dass Sie eine verkabelte Infrastruktur auf Bereiche erweitern können, in denen keine Kabel zur Verfügung stehen. So können die Benutzer mobil arbeiten oder an die verfügbaren Netzwerkressourcen angeschlossen bleiben.

Was möchten Sie tun?

- [Einstellen der Wireless-Funk-Parameter](#)
- [Einstellen der Parameter für Wireless-Sicherheit](#)
- [Bearbeiten des 'Wireless Status'](#)
- [Deaktivieren von Wireless-Verbindungen](#)

4.4.1. Einstellen der Wireless-Funk-Parameter:

4.4.1.1. Wählen Sie 'Radio Settings' auf der Seite 'Wireless'.

Die Seite 'Radio Settings' wird angezeigt wie in ABBILDUNG 4-7 dargestellt:

ABBILDUNG 4-7: Die Seite 'Wireless – Radio Settings'

4.4.1.2. Klicken Sie neben 'Wireless' auf 'Enable'.

4.4.1.3. Optional: Überprüfen Sie die Nummer der Firmware Version und die Datumsinformation Ihrer Version.

4.4.1.4. Geben Sie die folgenden Funk-Grundeinstellungen ein:

Größe	Beschreibung
Mode	<p>Wählt den Wireless-Modus, den Ihr Unternehmens-AP-Router unterstützt, aus der Dropdown-Liste.</p> <p>Die verfügbare Optionen sind 802.11B, 802.11G und MIXED, die sowohl 802.11B als auch 802.11G unterstützt.</p>
ESSID	<p>Geben Sie die eindeutige Identifikation für das Extended Service Set ein, das von Client-Stationen in einem Infrastruktur-Verbund gemeinsam verwendet wird, z.B. <i>WLAN-test</i>.</p>

	Hier ist auf Groß- und Kleinschreibung zu achten; 32 Zeichen dürfen nicht überschritten werden.
Channel	Wählt einen IEEE 802.11G-Kanal für Wireless LAN-Übertragungen aus der Dropdown-Liste. Bestimmt die Bandbreite, in der die Wireless-Übertragung arbeitet. AP und zugeordnete Client-Stationen arbeiten in einem der Kanäle von 1 bis 14.

4.4.1.5. Geben Sie die folgenden, erweiterten Funkparameter ein:

Größe	Beschreibung
Beacon Interval	Geben Sie das Zeitintervall in Millisekunden zwischen vom AP (Access Point) übertragenen Beacons in das Feld Beacon Interval ein, z.B. 100.
RTS Threshold	Geben Sie eine Zahl in das Feld RTS Threshold ein. Wird auch 'Request-to-Send Threshold' genannt. Dieses Feld bestimmt die minimale Größe von Daten-Frames, über der das RTS-Protokoll verwendet wird; der Bereich reicht von 256 bis 2432. RTS hilft, Datenkollisionen von versteckten Knoten zu verhindern.
Fragmentation Threshold	Geben Sie eine Zahl in das Feld Fragmentation Threshold ein. Für bessere Effizienz bei hohen Datentransferraten werden große Dateien in Fragmente zerlegt. Dieses Feld gibt die voreingestellte Paketgröße an, eine gerade Zahl aus dem Bereich von 256 bis 2346.
DTIM Interval	Geben Sie eine Zahl in das Feld DTIM Interval ein. Wird auch Delivery Traffic Indication Map genannt. Dieses Feld bestimmt die Anzahl der Beacon-Intervalle zwischen aufeinanderfolgenden DTIMs; Wertebereich von 1 bis 255.
Preamble Type	Wählen Sie entweder Short Preamble (72 bits) oder Long Preamble (144 bits).
Distribution System	Wenn Sie auf Ihrem Router ein Wireless Distribution System verwenden möchten, klicken Sie auf Enable neben Distribution System und geben Sie dann die physischen Adressen der Client-PCs ein, wie in Schritt 6 beschrieben.

Andernfalls klicken Sie auf Disable.

Hinweis :

Die Voreinstellungen der obigen erweiterten Wireless-Einstellungen sind auf der rechten Seite dargestellt. Wenn Sie nicht wissen, wie Sie diese Einstellungen ändern müssen, lassen Sie sie wie in Abbildung 4-8 dargestellt:

Default Values for Radio Settings	
Beacon Interval	100
RTS Threshold	2432
Fragmentation Threshold	2346
DTIM Interval	1
Preamble Type	Long Preamble
Distribution System	Disable

ABBILDUNG 4-8: Voreingestellte Werte für Funkeinstellungen

4.4.1.6. Optional: Wenn Sie 'Distribution System' aktiviert haben, geben Sie die physische Adressen der angeschlossenen Client-PCs in einem Wireless-Netzwerk in die in ABBILDUNG 4-9 gezeigten 'Peer AP MAC Address'-Felder 1-8 ein:

Distribution System:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Peer AP MAC Address 1:	<input type="text"/>
Peer AP MAC Address 2:	<input type="text"/>
Peer AP MAC Address 3:	<input type="text"/>
Peer AP MAC Address 4:	<input type="text"/>
Peer AP MAC Address 5:	<input type="text"/>
Peer AP MAC Address 6:	<input type="text"/>
Peer AP MAC Address 7:	<input type="text"/>
Peer AP MAC Address 8:	<input type="text"/>

ABBILDUNG 4-9: Peer AP MAC-Adressen für Distribution-Systeme

4.4.1.7. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

4.4.2. Einstellen der Parameter für Wireless-Sicherheit:

4.4.2.1. Klicken Sie auf 'Security Settings' auf der Seite 'Wireless'.

Die 'Security Settings' werden angezeigt wie in ABBILDUNG 4-10 dargestellt:

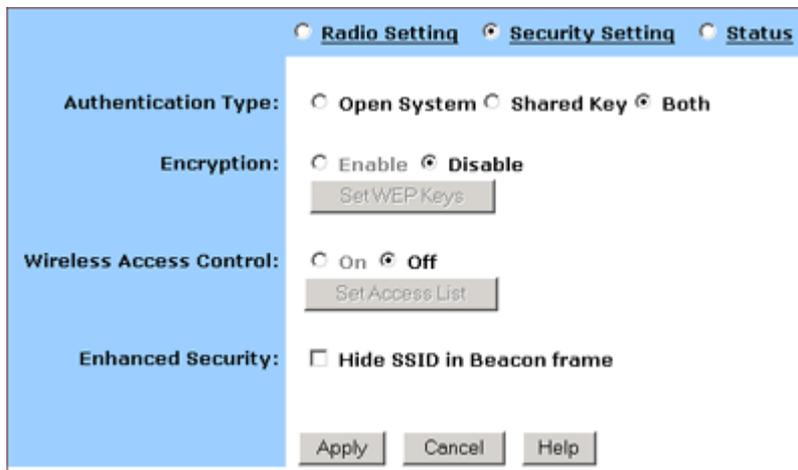


ABBILDUNG 4-10: Die Seite 'Wireless – Security Settings'

4.4.2.2. Wählen Sie *Open System*, *Shared Key* oder *Both* aus der Dropdown-Liste 'Authentication Type'.

Hinweise:

'Authentication Type' gibt einen Authentifizierungsalgorithmus an, der vom Access Point unterstützt wird:

'Open System': Der einfachste zur Verfügung stehende Authentifizierungsalgorithmus. Dieser ist im Grunde Null-Algorithmus. Jede Station, die mit diesem Algorithmus eine Authentifizierung anfordert, kann authentifiziert werden, wenn am Empfängerrechner Open System eingestellt ist.

'Shared Key' (gemeinsamer Schlüssel): Erlaubt Stationen mit bestimmten WEP-(Wired Equivalent Privacy)-Schlüsseln, authentifiziert zu werden.

'Both' (beide): Unterstützt die Authentifizierungen sowohl von Stationen, die einen gemeinsamen Schlüssel (shared key) kennen als auch solcher, die keinen kennen.

Wenn Sie verhindern möchten, dass andere Stationen ohne bestimmte WEP-(Wired Equivalent Privacy)-Schlüssel mit dem AP in Verbindung treten, wählen Sie 'Enable' neben 'Encryption' und klicken Sie auf 'Set WEP Keys', um die relevanten Schlüssel zu bestimmen; Ansonsten wählen Sie 'Disable'. Zu detaillierten Anweisungen zur Einstellung der WEP-Schlüssel siehe unter Einstellen der WEP Key.

Wenn Sie den Zugang zum Internet basierend auf den MAC (Media Access Control)-Adressen der Benutzer erlauben möchten, wählen Sie 'On' neben 'Wireless Access Control' und klicken Sie auf 'Set

Access List' um die relevanten MAC-Adressen festzulegen; Ansonsten klicken Sie auf 'Off'. Zu detaillierten Anweisungen zur Einstellung der relevanten MAC-Adressen siehe unter Einstellen der Wireless-Zugangskontroll.

- 4.4.2.3. Wählen Sie neben 'Enhanced Security' (höhere Sicherheit) entweder 'Enable' oder 'Disable'. Wenn Sie die Funktion 'Enhanced Security' aktivieren, weiter mit Schritt 6.
- 4.4.2.4. Optional: Wenn Sie 'Enhanced Security' aktiviert haben, können Sie wählen, Ihre SSID (Service Set Identifier) im Beacon Frame zu unterdrücken.
- 4.4.2.5. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

4.4.3. Einstellen der WEP Keys:

- 4.4.3.1. Aktivieren Sie 'Encryption' auf der Seite 'Security Settings' und klicken Sie auf 'WEP Keys'.

Die Seite 'WEP-Keys' wird angezeigt wie in ABBILDUNG 4-11 dargestellt:

The screenshot shows a configuration window for WEP keys. On the left, a blue sidebar contains the following labels: 'Encryption Level:', 'WEP Key Type:', 'Passphrase:', and 'Default TX Key:'. The main content area includes: 'Encryption Level: 64 Bit (selected) 128 Bit'; 'WEP Key Type: Automatic (selected) Manually'; 'Passphrase: [text input] [Generate]'; 'Key 1: [00000]', 'Key 2: [00000]', 'Key 3: [00000]', 'Key 4: [00000]'; 'Clear Keys' button; 'Default TX Key: [1]'; 'Apply' and 'Cancel' buttons.

ABBILDUNG 4-11: Das Fenster 'Set WEP Keys'

4.4.3.2. Wählen Sie *64 Bit* oder *128 Bit* neben 'Encryption Level'.

Hinweis:
128 Bit-Verschlüsselung bietet einen sichereren Algorithmus, verlangsamt jedoch die Übertragungsgeschwindigkeit Ihres Netzwerks.

4.4.3.3. Wenn Sie die WEP Keys automatisch generieren möchten, tun Sie Folgendes:

4.4.3.3.1. Wählen Sie 'Automatic' neben 'WEP Key Type'.

4.4.3.3.2. Geben Sie eine beliebige Zeichenfolge in das Feld 'Passphrase' ein und klicken Sie auf 'Generate'.

Vier neu erzeugte WEP Keys werden unter 'Key 1' – 'Key 4' angezeigt.

4.4.3.3.3. Optional: Klicken Sie auf 'Clear Keys', um alle Keys auf Null zurückzusetzen.

Hinweis:
Achten Sie darauf, die Passphrase-Zeichenfolge zu notieren, so dass Sie falls nötig darauf zurückgreifen können.

4.4.3.4. Wenn Sie die Key-Elemente manuell eingeben möchten, tun Sie das Folgende:

4.4.3.4.1. Wählen Sie 'Manually' neben 'WEP Key Type'.

4.4.3.4.2. Wenn Sie 'Alphanumeric: 5 characters' wählen, geben Sie jeweils eine Folge von 5 alphanumerischen Zeichen in die Felder 'Key 1' – 'Key 4' ein.

4.4.3.4.3. Wenn Sie 'Hexadecimal: 10 digits (0-9, A-F)' wählen, geben Sie jeweils eine Folge von 10 hexadezimalen Zeichen in die Felder 'Key 1' – 'Key 4' ein.

4.4.3.4.4. Optional: Klicken Sie auf 'Clear Keys', um alle Keys auf Null zurückzusetzen.

4.4.3.5. Wählen Sie die voreingestellte Verschlüsselung aus der Dropdown-Liste 'Default TX Key' z.B. 'Key 1'.

4.4.3.6. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

4.4.4. Einstellen der Wireless-Zugangskontrolle:

4.4.4.1. Schalten Sie auf der Seite 'Security Settings' die 'Wireless Access Control' auf 'On' und klicken Sie auf 'Set Access List'.

Das Fenster 'Wireless Control List' wird angezeigt wie in ABBILDUNG 4-12 dargestellt:

mac	Address
mac 1	000000000000
mac 2	000000000000
mac 3	000000000000
mac 4	000000000000
mac 5	000000000000
mac 6	000000000000
mac 7	000000000000
mac 8	000000000000
mac 9	000000000000
mac 10	000000000000
mac 11	000000000000

ABBILDUNG 4-12: Das Fenster 'Wireless Control List'

4.4.4.2. Geben Sie die MAC-Adressen ein, denen Sie Zugang zum Internet erlauben möchten. Sie können bis zu 80 MAC-Adressen in der Liste angeben.

4.4.4.3. Wenn Sie die Bearbeitung aller MAC-Adressen abgeschlossen haben, klicken Sie auf 'Submit', oder klicken Sie auf 'Cancel', um Ihre Änderungen zurückzusetzen.

4.4.4.4. Optional: Sie können auf 'Refresh' klicken, um die aktuellsten, freigegebenen MAC-Adressen anzuzeigen.

4.4.5. Bearbeiten des 'Wireless Status':

4.4.5.1. Wählen Sie 'Status' auf der 'Wireless'-Seite.

Die Seite 'Status' wird mit den AP-Funkstatistiken Ihres Gateways angezeigt, einschließlich *Status*, *Max.Mb/s*, *IP Addr*, *MAC Addr*, *Radio SSID*, *Receive data* und *Transmit data*. Siehe ABBILDUNG 4-13:

AP Radio			
<input type="button" value="Refresh"/>			
Status: up Max.Mb/s: 54 MBps IP Addr: 192.168.62.1 MAC Addr: 00:0a:15:00:00:02 Radio SSID: WLAN-test			
Receive		Transmit	
successful unicast frames	0	successful unicast frames	8
successful multicast frames	0	successful multicast frames	0
dropped frames	0	dropped frames	0
failed frames	0	failed frames	5
<input type="button" value="Display Association Table"/>		<input type="button" value="Help"/>	

ABBILDUNG 4-13: Die Seite 'Wireless – Status'

4.4.5.2. Um die Wireless-Geräte anzuzeigen, die der AP (Access Point) erkannt hat, klicken Sie auf 'Display Association Table'.

Index	Time	Mac Address	Add/Delete from Access List
1	None	None	None

4.4.5.3. Optional: Sie können auf 'Refresh' klicken, um die aktuellsten Daten anzuzeigen.

4.4.6. Deaktivieren von Wireless-Verbindungen:

4.4.6.1. Wählen Sie 'Radio Settings' auf der Seite 'Wireless'.

Die Seite 'Radio Settings' wird angezeigt wie in ABBILDUNG 4-7 dargestellt.

Wenn Sie nicht möchten, dass der Router Wireless-Verbindungen unterstützt, wählen Sie 'Disable' (deaktivieren).

Hinweis :
Keine der Wireless-Funktionen des Routers funktioniert, bevor Sie diese aktivieren.

4.5 Tools

Auf der Seite 'Tools' können Sie:

- **Das Administrator-Passwort für Ihren Router ändern**
- **Wiederherstellen der werksseitig voreingestellten Konfiguration**
- **Zurücksetzen des Gateway**
- **Aktualisieren der Firmware**

! Wichtig:

Wir empfehlen dringend, das Administratorpasswort beim ersten Login zu ändern.

Wiederherstellen der werksseitigen Voreinstellungen setzt alle Router-Konfigurationen auf jeder Seite zurück; wir empfehlen daher, eine Sicherungskopie der Gateway-Konfigurationsdaten mit Hilfe der DOS-Befehle auf Ihrem PC zu erstellen. Außerdem können Sie die werksseitigen Voreinstellungen im DOS-Fenster wiederherstellen. Zu detaillierten Anweisungen siehe **To Backup or Restore the Configuration Data Using DOS Commands**.

Wenn Sie die Hardware zurücksetzen möchten, müssen Sie das Gateway zurücksetzen.

Bevor Sie die Firmware aktualisieren, müssen Sie das Firmware Image File von der Gateway Website herunter und es auf Ihrem lokalen Root-Laufwerk speichern.

4.5.1. Das Administrator-Passwort für Ihren Router ändern:

4.5.1.1. Klicken Sie in der Navigationsleiste auf 'Tools'.

Die Seite 'Tools' wird angezeigt wie in ABBILDUNG 4-14 dargestellt:

Change Password:	Old Password:	<input type="text"/>
	New Password:	<input type="text"/>
		(* Maximum 31 characters)
	Confirm Password:	<input type="text"/>
	<input type="button" value="Apply"/>	<input type="button" value="Cancel"/> <input type="button" value="Help"/>
Restore Factory Defaults:	<input type="button" value="Restore to Default"/>	<input type="button" value="Backup/Restore Help"/>
Reset Gateway:	<input type="button" value="Reset"/>	
Upgrade Firmware:	<input type="text"/>	<input type="button" value="Browse..."/> <input type="button" value="Upgrade now"/> <input type="button" value="Help"/>

ABBILDUNG 4-14: Die Seite 'Tools'

4.5.1.2. Geben Sie das alte Passwort in das Feld 'Old Password' ein. Das voreingestellte Passwort ist *1234*.

4.5.1.3. Geben Sie ein neues Passwort in das Feld 'New Password' ein.

Hinweis:
Das Passwort muss kürzer als 64 Zeichen sein..

4.5.1.4. Geben Sie das neue Passwort in das Feld 'Confirm Password' ein.

4.5.2. Wiederherstellen der werksseitig voreingestellten Konfiguration:

4.5.2.1. Klicken Sie auf der Seite 'Tools' neben 'Restore Factory Defaults' auf 'Restore to Default' (Voreinstellungen wiederherstellen).

Eine Warnung wird angezeigt, siehe ABBILDUNG 4-15:



ABBILDUNG 4-15: Dialogfeld-Warnung

4.5.2.2. Klicken Sie auf 'OK'.

Wichtig:

Wiederherstellen der werksseitigen Voreinstellungen setzt alle Router-Konfigurationen auf jeder Seite zurück; wir empfehlen daher, vorher eine Sicherungskopie der Gateway-Konfigurationsdaten mit Hilfe der DOS-Befehle auf Ihrem PC zu erstellen. Zu Details siehe Erstellen einer Sicherungskopie oder Wiederherstellen der Konfigurationsdaten mit DOS-Befehlen.

Außerdem können Sie die werksseitigen Voreinstellungen mit DOS-Befehlen wiederherstellen. Zu detaillierten Anweisungen siehe Erstellen einer Sicherungskopie oder Wiederherstellen der Konfigurationsdaten mit DOS-Befehlen.

4.5.3. Erstellen einer Sicherungskopie oder Wiederherstellen der Konfigurationsdaten mit DOS-Befehlen:

Zum Erstellen einer Sicherungskopie der Konfigurationsdaten vom Gateway auf ihren PC funktioniert das Gateway als TFTP-Server.

Zum Erstellen von Sicherungskopien der Konfigurationsdaten verwenden Sie im DOS-Fenster den folgenden Befehl:

```
tftp -i gateway_Ip_address GET filename
```

Zum Wiederherstellen der Konfigurationsdaten verwenden Sie im DOS-Fenster den folgenden Befehl:

```
tftp -i gateway_Ip_address PUT filename
```

gateway_Ip_address: Die IP-Adresse des Gateway, auf dem Sie die Sicherungskopie der Konfigurationsdaten speichern möchten.

filename: Der Dateiname für die Sicherungskopie auf dem Gateway.
Er muss mit *“nvram”*, beginnen, wobei die Groß- und Kleinschreibung keine Rolle spielt, z.B. *“nvram__11032003”*.

4.5.4. Zurücksetzen des Gateway:

Wenn Sie die Hardware zurücksetzen möchten, klicken Sie auf 'Reset Gateway' auf der Seite 'Tools'.

4.5.5. Aktualisieren der Firmware:

4.5.5.1. Laden Sie ein Firmware Image von der Gateway Website herunter und speichern Sie es auf Ihrem lokalen Root-Laufwerk.

4.5.5.2. Geben Sie den Dateipfad und den Dateinamen in das Feld 'Upgrade Firmware' ein, klicken Sie auf 'Browse' um das Dialogfeld 'Choose file' (Datei wählen) zu öffnen, siehe ABBILDUNG 4-15:

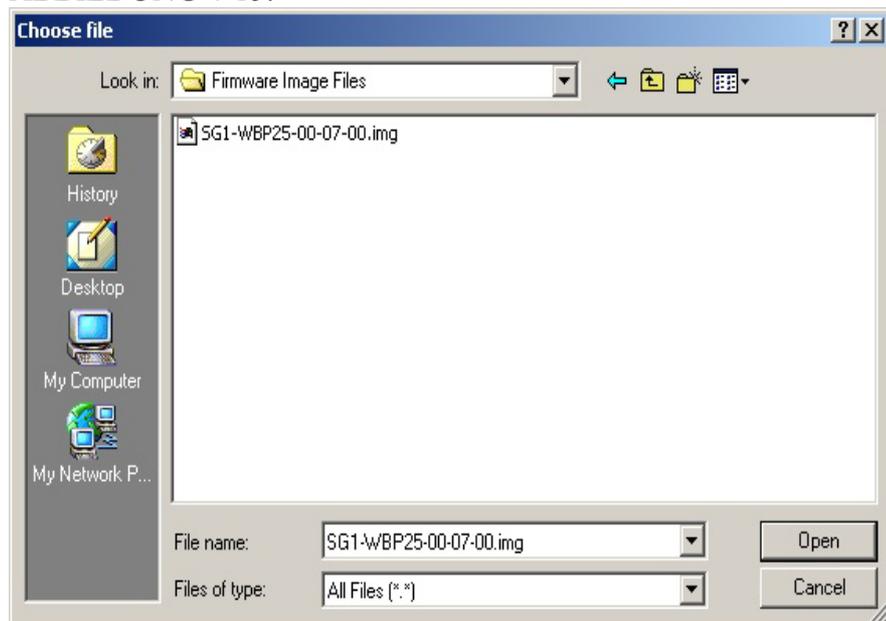


ABBILDUNG 4-15: Das Dialogfeld 'Chose File' zum Aktualisieren der Firmware

4.5.5.3. Wählen Sie die heruntergeladene Firmware und klicken Sie auf 'Open'.

4.5.5.4. Das Dialogfeld 'Choose File' wird geschlossen.

4.5.5.5. Klicken Sie jetzt auf 'Upgrade'. Die Firmware des Geräts wird aktualisiert.

Vorsicht :

**Die Aktualisierung der Firmware dauert ungefähr 10 Sekunden;
Schalten Sie das Gerät währenddessen bitte NICHT aus.**

4.6 Status

Auf der Seite 'Status' werden die aktuellsten Informationen über Ihren Router angezeigt und alle 10 Sekunden aktualisiert, z.B. *Host Name, Domain, PPPoE Login, LAN/WAN* and *DDNS Status*.

Unterschiedliche Konfigurationen können zur Anzeige verschiedener Daten führen; vergleichen Sie hierzu die

Hinweis :

Wenn Sie die Konfiguration ändern möchten, gehen Sie zur Seite 'Setup'. Zu detaillierten Anweisungen siehe [Setup](#).

Abbildungen 3-16 und 4-17.

- Wenn Sie 'PPPoE Login' aktiviert haben, wird die Seite 'Status' angezeigt wie in **ABBILDUNG 4-16**:

Host Name:	StartGate
Domain:	xyz.isp.com
PPPoE Login:	Enabled Status: Disconnected
	<input type="button" value="Connect"/>
LAN:	
	IP Address: 192.168.62.1
	Subnet Mask: 255.255.255.0
WAN:	Dynamic
	IP Address: 0.0.0.0
	Subnet Mask: 255.0.0.0
	Default Gateway: 255.255.255.255
	DNS: 0.0.0.0
	0.0.0.0
	0.0.0.0
DDNS Status:	
	Server: The service is disabled
	Status: The account is not set yet.
	<input type="button" value="Help"/>

ABBILDUNG 4-16: Die Seite 'Status' mit aktiviertem 'PPPoE Login'

- Wenn Sie 'Dynamic IP' gewählt und 'PPPoE LOGIN' deaktiviert haben, wird die Seite 'Status' angezeigt wie in **ABBILDUNG 4-17**:

▪

Host Name:	StartGate	
Domain:	xyz.isp.com	
PPPoE Login:	Disabled	
LAN:		
	IP Address:	192.168.62.1
	Subnet Mask:	255.255.255.0
WAN:	Dynamic	
	IP Address:	0.0.0.0
	Subnet Mask:	255.0.0.0
	Default Gateway:	255.255.255.255
	DNS:	0.0.0.0
		0.0.0.0
		0.0.0.0
	<input type="button" value="DHCP Release"/>	<input type="button" value="DHCP Renew"/>
DDNS Status:		
	Server:	The service is disabled
	Status:	The account is not set yet.
	<input type="button" value="Help"/>	

ABBILDUNG 4-17: Die Seite 'Status' mit deaktiviertem 'PPPoE Login'

Hinweise:

Wenn Sie 'Dynamic IP' gewählt und 'PPPoE LOGIN' deaktiviert haben, werden die Tasten 'DHCP Release' und 'DHCP Renew' angezeigt:

Um die aktuellste WAN IP-Adresse freizugeben, klicken Sie auf 'DHCP Release'.

Um die aktuellste WAN IP-Adresse zu erneuern, klicken Sie auf 'DHCP Renew'.

Status-Details:

Größe	Beschreibung
Hostname	Zeigt den Namen des Geräts an.
Domain	Zeigt den Domain-Namen des Geräts an.
PPPoE Login	Zeigt den aktuellen PPPoE Login-Status an: <ul style="list-style-type: none"> ▪ Disabled (Deaktiviert) ▪ Enabled (Aktiviert): 'Connected', 'Connecting' oder 'Disconnected'.

LAN	Zeigt die aktuelle IP Address und Subnet Mask des Geräts an, wie Sie von Nutzern in Ihrem internen Netzwerk gesehen werden.
WAN	Zeigt die IP Address, Subnet Mask, Default Gateway und DNS des Routers an, wie sie von externen Nutzern im Internet gesehen werden.
DDNS	Zeigt den Dynamic DNS-Server und den Status an. Wenn Sie die Einstellung ändern möchten, gehen Sie zur Seite 'Advanced Dynamic DNS'. Zu detaillierten Anweisungen siehe <u>To Configure a Dynamic DNS Server</u>.

4.7 DHCP

Auf der Seite 'DHCP' können Sie Ihr NAT/Firewall Gateway als einen DHCP-(Dynamic Host Configuration Protocol)-Server einstellen; DHCP-Server weisen allen Client-PCs in Ihrem Netzwerk automatisch IP-Adressen zu.

Notes

Wenn Sie DHCP aktivieren möchten, achten Sie darauf, dass nicht bereits ein DHCP-Server auf Ihrem Router eingerichtet ist.

Wenn Sie DHCP auf Ihrem Router nicht aktivieren möchten, müssen Sie jedem PC in Ihrem Netzwerk manuell eine Adresse zuweisen;

Wenn Sie DHCP aktivieren, achten Sie darauf, dass jeder PC dafür konfiguriert ist, automatisch eine IP-Adresse zu erhalten.

Was möchten Sie als nächstes tun?

- Einstellen des Routers als DHCP-Server
- Anzeigen der 'Active IP Table'
- DHCP auf Ihrem Router deaktivieren

4.7.1. Einstellen des Routers als DHCP-Server:

4.7.1.1. Achten Sie darauf, dass nicht bereits ein DHCP-Server auf Ihrem Router eingerichtet ist.

4.7.1.2. Achten Sie darauf, dass jeder PC in Ihrem Netzwerk dafür konfiguriert ist, automatisch eine IP-Adresse zu erhalten.

4.7.1.3. Klicken Sie in der Navigationsleiste auf 'DHCP'.

Die Seite 'DHCP' wird angezeigt wie in ABBILDUNG 4-18 dargestellt:

DHCP Server: Enable Disable

IP Pool Starting Address: 192.168.62.50

IP Pool Ending Address: 192.168.62.100

Lease Time: 24 Hours.

Display DHCP Table

Apply Cancel Help

ABBILDUNG 4-18: Die Seite 'DHCP'

- 4.7.1.4. Klicken Sie neben 'DHCP Server' auf 'Enable'.
- 4.7.1.5. Geben Sie eine 'IP Pool Starting Address' ein, um die erste IP-Adresse zu bestimmen, die einem PC in Ihrem Netzwerk zugewiesen werden kann.
- 4.7.1.6. Geben Sie eine 'IP Pool Ending Address' ein, um die letzte IP-Adresse zu bestimmen, die einem PC in Ihrem Netzwerk zugewiesen werden kann.
- 4.7.1.7. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

4.7.2. DHCP auf Ihrem Router deaktivieren:

- 4.7.2.1. Klicken Sie auf der Seite 'DHCP' neben 'DHCP Server' auf 'Disable'.
- 4.7.2.2. Klicken Sie auf 'Apply'.

4.7.3 Anzeigen der 'Active IP Table':

Wenn Sie Information über PCs, denen vom DHCP-Server Adressen zugewiesen wurden, anzeigen möchten, klicken Sie auf 'Display DHCP Table'.

Für jeden aktiven Client-PC werden *DHCP Server IP Address*, *Client Host Name*, *IP Address* und *MAC Address* in der Tabelle aufgelistet; siehe ABBILDUNG 4-19:

DHCP Active IP Table			
DHCP Server IP Address:			192.168.62.1
Index	Client Host Name	IP Address	MAC Address
1	swlab2	192.168.62.51	00:06:5b:a5:7b:59

ABBILDUNG 4-19: DHCP Active IP Table

Optional: Sie können auf 'Refresh' klicken, um die aktuellsten Daten zu erhalten.

Hinweis:

Wenn Sie die DMZ- und LAN-Funktionen aktiviert haben, können Sie die relevanten Informationen auch in der DHCP Active IP Table für die DMZ-Zone und in der DHCP Active IP Table für das LAN finden.

4.8 Log

Auf der Seite 'Log' können Sie 'Access Log' einstellen und Log-Dateien ansehen, die die Zugangsaktivität von LAN und WAN-Client-PCS aufzeichnen, einschließlich *Session Event Log*, *Block Event Log*, *Intrusion Event Log* und *Wireless Event Log*.

Was möchten Sie tun?

- [Access Log auf Ihrem Router einstellen](#)
- [Löschen von DMZ Hosts](#)
- ['Block Event Log' anzeigen](#)
- ['Intrusion Event Log' anzeigen](#)
- ['Wireless Event Log' anzeigen](#)

4.8.1. Access Log auf Ihrem Router einstellen:

4.8.1.1. Klicken Sie in der Navigationsleiste auf 'Log'.

Die Seite 'Log' wird angezeigt wie in ABBILDUNG 4-20 dargestellt:

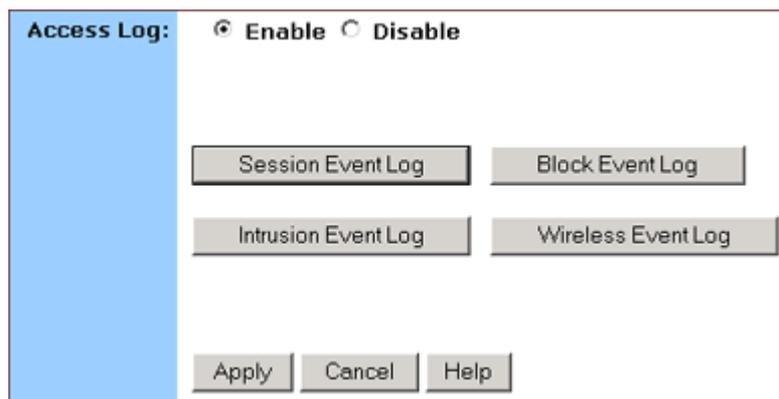


ABBILDUNG 4-20: Die Seite 'Log'

4.8.1.2. Wählen Sie 'Enable'.

4.8.1.3. Klicken Sie auf 'Apply' oder auf 'Cancel', um Ihre Änderungen zurückzunehmen.

4.8.2. 'Session Event Log' anzeigen:

4.8.2.1. Klicken Sie auf 'Session Event Log' auf der Seite 'Log'.

Die 'Session Event Log Table' wird angezeigt, die alle Session Event Entry-Informationen enthält, wie z.B. *Record Name, Transport type, Source IP* etc., siehe ABBILDUNG 4-21:

Session Event Log Table							
						Clear	Refresh
Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2003.11.06 03:34:22	ICMP	61.173.63.220	0:8	61.171.242.88	0:0	POLICY_MIGRATION
2	2003.11.06 03:34:45	ICMP	218.80.56.153	0:8	61.171.242.88	0:0	POLICY_MIGRATION
3	2003.11.06 03:34:38	UDP	61.171.242.88	123	192.5.41.40	123	POLICY_MIGRATION
4	2003.11.06 03:35:49	ICMP	61.172.27.50	0:8	61.171.242.88	0:0	TIMBOUT
5	2003.11.06 03:36:41	ICMP	61.172.104.82	0:8	61.171.242.88	0:0	TIMBOUT

ABBILDUNG 4-21: Session Event Log Table

4.8.2.2. Optional: Sie können auf 'Refresh' klicken, um die aktuellsten Daten zu erhalten.

4.8.2.3. Optional: Klicken Sie auf 'Clear' um alle Log-Informationen zu löschen.

4.8.3. 'Block Event Log' anzeigen:

4.8.3.1. Klicken Sie auf 'Block Event Log' auf der Seite 'Log'.

Die 'Block Event Log Table' wird angezeigt, die alle Block Event Entry-Informationen enthält, z.B. *Record Name, Transport type, Source IP*, etc., siehe ABBILDUNG 4-22:

Block Event Log Table							
						Clear	Refresh
Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2003.11.06 03:34:46	TCP	218.80.56.153	3820	61.171.242.88	135	Default Defense
2	2003.11.06 03:34:52	TCP	218.80.56.153	3820	61.171.242.88	135	Default Defense
3	2003.11.06 03:35:01	TCP	61.171.212.54	3196	61.171.242.88	445	Default Defense
4	2003.11.06 03:35:04	TCP	61.171.212.54	3196	61.171.242.88	445	Default Defense
5	2003.11.06 03:36:00	TCP	195.117.228.35	4066	61.171.242.88	2098	Default Defense

ABBILDUNG 4-22: Block Event Log Table

4.8.3.2. Optional: Sie können auf 'Refresh' klicken, um die aktuellsten Daten zu erhalten.

4.8.3.3. Optional: Klicken Sie auf 'Clear' um alle Log-Informationen zu löschen.

4.8.4. 'Intrusion Event Log' anzeigen:

4.8.4.1. Klicken Sie auf 'Intrusion Event Log' auf der Seite 'Log'.

Die 'Intrusion Event Log Table' wird angezeigt, die alle Intrusion Event-Einträge enthält: *Record Name* und *Intrusion Type*, siehe ABBILDUNG 4-23:



Intrusion Event Log Table			Clear	Refresh
Index	Record Time	Intrusion Type		
1	None	None		

ABBILDUNG 4-23: Intrusion Event Log Table

4.8.4.2. Optional: Sie können auf 'Refresh' klicken, um die aktuellsten Daten zu erhalten.

4.8.4.3. Optional: Klicken Sie auf 'Clear' um alle Log-Informationen zu löschen.

4.8.5. 'Wireless Event Log' anzeigen:

4.8.5.1. Klicken Sie auf 'Wireless Event Log' auf der Seite 'Log'.

Die 'Session Event Log Table' wird angezeigt, die alle Wireless Event-Einträge enthält: *Time*, *Severity* und *Description*, siehe ABBILDUNG 4-24:

Wireless Event Log Table			
Index	Time	Severity	Description
1	2003.11.06 03:33:10	Info	WLAN zone information is not set
2	2003.11.06 03:33:11	Info	WLAN Access Point started
3	2003.11.06 03:49:42	Info	WLAN zone information is not set
4	2003.11.06 03:49:42	Info	WLAN Access Point started
5	2003.11.06 03:50:42	Info	WLAN zone information is not set
6	2003.11.06 03:50:42	Info	WLAN Access Point started
7	2003.11.06 03:51:42	Info	WLAN zone information is not set
8	2003.11.06 03:51:42	Info	WLAN Access Point started
9	2003.11.06 03:52:12	Info	WLAN zone information is not set
10	2003.11.06 03:52:12	Info	WLAN Access Point started

ABBILDUNG 4-24: Wireless Event Log Table

4.8.5.2. Optional: Sie können auf 'Refresh' klicken, um die aktuellsten Daten zu erhalten.

4.8.5.3. Optional: Klicken Sie auf 'Clear' um alle Log-Informationen zu löschen.

4.8.6. Access Log auf Ihrem Router deaktivieren:

4.8.6.1. Klicken Sie auf der Seite 'Log' neben 'Access Log' auf 'Disable'.

4.8.6.2. Klicken Sie auf 'Apply'.

4.9 Statistiken

Auf der Seite 'Statistics' können Sie Statistikinformationen über LAN, WAN und AP (Access Point)-Funkanschlüsse, einschließlich *Status*, *Max.Mb/s*, *IP Addr* und *MAC Addr*, *Receive data* und *Transmit data* einsehen.

Sie können in der Navigationsleiste auf 'Statistics' klicken; die Seite 'Statistics' wird angezeigt wie in ABBILDUNG 4-25:

LAN WAN AP			
LAN Statistics			
Refresh			
Status: up Max.Mb/s: 100.0 IP Addr: 192.168.62.1 MAC Addr: 00:0a:15:00:00:00			
Receive		Transmit	
total bytes	180771	total bytes	2673637
unicast pkts	4542	unicast pkts	2001
multicast pkts	160	multicast pkts	1764
discards	0	discards	0
errors	0	errors	0
unknown protocols	901	packets queued	0
WAN Statistics			
Refresh			
Status: up Max.Mb/s: 100.0 IP Addr: 0.0.0.0 MAC Addr: 00:0a:15:00:00:01			
Receive		Transmit	
total bytes	0	total bytes	1800
unicast pkts	0	unicast pkts	0
multicast pkts	0	multicast pkts	30
discards	0	discards	0
errors	0	errors	0
unknown protocols	0	packets queued	0
AP Radio			
Refresh			
Status: up Max.Mb/s: 54 MBps IP Addr: 192.168.62.1 MAC Addr: 00:0a:15:00:00:02 Radio SSID: WLAN-test			
Receive		Transmit	
successful unicast frames	0	successful unicast frames	9
successful multicast frames	0	successful multicast frames	0
dropped frames	0	dropped frames	0
failed frames	0	failed frames	3

ABBILDUNG 4-25: Die Seite 'Statistics'

4.9.1. Die Seite 'Statistics' enthält drei Teile:

4.9.1.1. 'LAN Statistics': Listet die Daten des LAN-Anschlusses auf.

4.9.1.2. 'WAN Statistics': Listet die Daten des WAN-Anschlusses auf.

4.9.1.3. 'AP Radio': Listet die Daten des Access Point-Funks auf.

Hinweis:

Sie können in jedem der obigen Teile auf 'Refresh' klicken, um die aktuellsten Daten zu erhalten.

5. Erweiterte Funktion

In diesem Kapitel erfahren Sie, wie die erweiterten Administrativfunktionen, die der Unternehmens-AP-Router bereitstellt, einschließlich Virtuellem Server, Filtern, IP/URL Block, Speziellen Anwendungen, DMZ Host, MAC Clone, Dynamic DNS, Proxy DNS und SNMP, verwendet werden.

Das Web-basierte Administrations-Tool bietet in der Navigationsleiste 'Advanced Function' einige erweiterte Dienste wie Filtern und Klonen Ihrer MAC-Adressen an.

In den meisten Fällen reichen die Grundfunktionen aus. Wenn Sie die erweiterte Konfiguration einstellen möchten, müssen Sie zuerst auf die Navigationsleiste 'Advanced Function' umschalten.

5.1. Umschalten zwischen Grundfunktionen und erweiterten Funktionen:

- 5.1.1. Um in das Fenster 'Advanced' zu schalten, klicken Sie auf 'Advanced' auf der rechten Seite des Fensters 'Basic', siehe ABBILDUNG 5-1:



ABBILDUNG 5-1: 'Basic'-Taste im Fenster 'Advanced'

- 5.1.2. Wenn Sie sich bereits im Fenster 'Advanced' befinden, klicken Sie auf 'Basic' auf der rechten Seite des Fensters, um so zum Fenster 'Basic' zurückzukehren; siehe ABBILDUNG 5-2:



ABBILDUNG 5-2: 'Basic'-Taste im Fenster 'Advanced'

5.2 Virtuelle Server

Sie können für bestimmte Situationen Internetnutzern den Zugang zu den Servern Ihres LANs ermöglichen, z.B. dem FTP Server, Telnet Server oder Web Server. Solche Remote-Dienste werden durch das Einrichten *Virtueller Server* geleistet.

Jeder virtueller Server hat seine eigene IP-Adresse und teilt sich eine einzige öffentliche IP-Adresse. Er wird durch den Protokolltyp (*TCP*, *UDP* oder *Both*) und eine TCP/UDP/Both-Portnummer definiert. Remote-Teilnehmer können über das Internet nur auf die virtuellen Server zugreifen, die auch aktiviert sind.

Hinweis:

Das Konfigurieren virtueller Server kann zum automatischen Erstellen von Filtern auf der Seite 'Filter' führen.

Was möchten Sie tun?

- Einrichten eines Client-PCs als virtuellen Server im LAN
- Entfernen virtueller Server aus dem LAN

5.2.1. Einrichten eines Client-PCs als virtuellen Server im LAN:

5.2.1.1. Klicken Sie auf 'Virtual Servers' in der Navigationsleiste 'Advanced'.

Die Seite 'Virtual Servers' erscheint mit einer Liste bestehender virtueller Server, siehe ABBILDUNG 5-3:

Service	Public IP Address	Public Port	Private Port	Protocol	Private IP Address
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0
<input type="text"/>	0.0.0.0	0	0	TCP	192.168.62.0

ABBILDUNG 5-3: Seite 'Virtual Servers'

5.2.1.2. Wenn Sie die DMZ aktiviert haben und Ihr Gateway nicht so konfiguriert ist, dass es automatisch eine IP-Adresse abrufen, wählen Sie eine der folgenden Optionen aus der 'Choose Interface'-Dropdown-Liste:

- (1) Extern – Intern: Einrichten virtueller Server in Ihrem LAN-Netzwerk.
- (2) Extern – DMZ: Einrichten virtueller Server in Ihrem DMZ-Netzwerk.

5.2.1.3. Wenn Sie das Betriebssystem Windows XP benutzen, müssen Sie einen Namen für den Remote-Dienst in das 'Service'-Feld

Hinweis:

Dies gilt nur für Client-PCs mit Windows XP. Da Windows XP die UPnP- (Universal Plug and Play) Funktion des Unternehmens-AP-Routers ausnutzt, ermöglicht es UPnP-unterstützenden Client-PCs die automatische Identifizierung des Routers.

eingeben.

5.2.1.4. Wählen Sie eine 'Public IP Address' aus der Dropdown-Liste.

Hinweis :

Die IP-Adresse eines DMZ Hosts erscheint nicht in der Liste.

Geben Sie eine Portnummer in die 'Public Port'- und 'Private Port'-Felder ein, z.B. 80 für HTTP. Hilfe bei der Auswahl eines Ports bieten die 'Well-known Ports' rechts auf der Seite; siehe ABBILDUNG 5-4:

Well-known Ports	
7	Echo
21	FTP
23	TELNET
25	SMTP
53	DNS
79	finger
80	HTTP
110	POP3
113	auth
119	NNTP
161	SNMP
162	SNMP Trap
1723	PPTP

ABBILDUNG 5-4: Bekannte Ports

Hinweise:

'Public Port' ist die TCP/UDP/Both-Portnummer, die von dem Server-PC im WAN benutzt wird. Sie wird auch externe Portnummer genannt, da diese Portnummer für Nutzer des Internets sichtbar ist.

'Private Port' ist die TCP/UDP/Both-Portnummer, die von dem Server-PC im LAN benutzt wird. Der festgelegte Public Port wird in diese interne Portnummer umgewandelt.

5.2.1.5. Wählen Sie zwischen *TCP*, *UDP* oder *Both* aus der 'Protocol'-Dropdown-Liste.

5.2.1.6. Geben Sie eine lokale IP-Adresse des Server-PCs im LAN in das 'Private IP Address'-Feld ein.

5.2.1.7. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.2.2. Entfernen virtueller Server aus dem LAN:

5.2.2.1. Klicken Sie auf 'Virtual Servers' in der Navigationsleiste 'Advanced'.

Eine Liste bestehender virtueller Server erscheint.

5.2.2.2. Wählen Sie für jeden virtuellen Server, den Sie entfernen möchten, *0.0.0.0* aus der 'Public IP Address'-Dropdown-Liste.

5.2.2.3. Klicken Sie auf 'Apply'.

5.3 Filter

Auf der Seite 'Filter' können Sie Filter einrichten, die ein- und ausgehenden Verkehr mit Ihrem Netzwerk selektiv zulassen können. Der Unternehmens-AP-Router wird Ihnen mit neun werksseitig eingerichteten Filtern geliefert.

Zusätzlich zu den neun voreingestellten Filtern können einige Filter automatisch erstellt werden, die das Funktionieren der virtuellen Server oder speziellen Anwendungen ermöglichen.

Es wird unbedingt empfohlen, zum Einrichten neuer Filter eine freie Zeile zu wählen, da Überschreiben oder Löschen von Filtern zum Deaktivieren einiger Dienste führen kann, z.B. wird Ihren Client-PCs dann der Internetzugang verwehrt.

Hinweis - Wenn Sie voreingestellte Filter überschrieben oder gelöscht haben, können Sie sie später mit der Funktion 'Restore Factory Defaults' auf der Seite 'Tools' abrufen. Zu detaillierten Anweisungen siehe Wiederherstellen der werksseitig voreingestellten Konfiguration.

Was möchten Sie tun?

- Einrichten eines Port-Filters oder Raw-IP-Filters
- Löschen von Filtern

5.3.1. Einrichten eines Port-Filters oder Raw-IP-Filters:

5.3.1.1. Klicken Sie auf 'Filter' in der Navigationsleiste 'Advanced'.

Die Seite 'Filter' erscheint, siehe **ABBILDUNG 5-5:**

Filtering Page:

ID	Filtering Layer	Proto Num	Direction	Private Port Range	Protocol
1	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="21"/> - <input type="text" value="21"/>	<input type="text" value="TCP"/>
2	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="1720"/> - <input type="text" value="1720"/>	<input type="text" value="TCP"/>
3	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="80"/> - <input type="text" value="80"/>	<input type="text" value="TCP"/>
4	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="53"/> - <input type="text" value="53"/>	<input type="text" value="UDP"/>
5	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="25"/> - <input type="text" value="25"/>	<input type="text" value="TCP"/>
6	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="110"/> - <input type="text" value="110"/>	<input type="text" value="TCP"/>
7	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="1503"/> - <input type="text" value="1503"/>	<input type="text" value="TCP"/>
8	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Outbound"/>	<input type="text" value="443"/> - <input type="text" value="443"/>	<input type="text" value="TCP"/>
9	<input type="text" value="Raw IP"/>	<input type="text" value="1"/>	<input type="text" value="Both"/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="TCP"/>
10	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Inbound"/>	<input type="text" value="8080"/> - <input type="text" value="8080"/>	<input type="text" value="TCP"/>
11	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Inbound"/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="TCP"/>
12	<input type="text" value="Port Filtering"/>	<input type="text" value="0"/>	<input type="text" value="Inbound"/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="TCP"/>

NAT: Enable Disable
 Firewall: Enable Disable
 Remote Management: Enable Disable
 IPSec Pass Through: Enable Disable
 PPTP Pass Through: Enable Disable
 Intrusion Detection: Enable Disable

ABBILDUNG 5-5: Seite 'Filter'

5.3.1.2. Wählen Sie eine Option aus der Dropdown-Liste der Seite 'Filtering': 1~12, 13~24, 25~36.

5.3.1.3. Wenn Sie 'Port Filtering' aus der Dropdown-Liste 'Filtering Layer' auswählen, müssen Sie folgende Einstellungen vornehmen:

5.3.1.3.1. Wählen Sie eine Verkehrsrichtung aus der Dropdown-Liste: *Inbound*, *Outbound* oder *Both*.

5.3.1.3.2. Geben Sie die Anfangs- und End-Portnummern, die Sie zulassen wollen, in die Felder des 'Private Port Range' ein.

5.3.1.3.3. Wählen Sie die Art des Protokolls aus der Dropdown-Liste: *TCP*, *UDP* oder *Both*.

5.3.1.4. Wenn Sie 'Raw IP' aus der Dropdown-Liste 'Filtering Layer' auswählen, müssen Sie folgende Einstellungen vornehmen:

Hinweis - Es steht der Bereich von 0 bis 255 zur Verfügung, jedoch nicht 6 (TCP) oder 17 (UDP); andernfalls wird dieser Portfilter nicht funktionieren.

5.3.1.4.1. Geben Sie eine IP-Protokollnummer in das Feld 'Proto Num' ein.

5.3.1.4.2. Wählen Sie eine Verkehrsrichtung aus der Dropdown-Liste: *Inbound*, *Outbound* oder *Both*.

5.3.1.4.3. Wählen Sie eine Option aus der 'Protocol'-Dropdown-Liste: *TCP*, *UDP* oder *Both*.

5.3.1.5. Optional: Wählen Sie 'Aktivieren' oder 'Deaktivieren' für folgende zusätzliche Filteroptionen:

Größe	Beschreibung
NAT	Ermöglicht das Einrichten einer NAT (Network Access Translation).
Firewall	Ermöglicht Ihnen, Ihr Netzwerk mit einer Firewall zu schützen.
Remote Management	Ermöglicht Ihnen den Zugang zum Web-basierten Administrations-Tool Ihres Routers mit Hilfe Ihrer WAN-Verbindung.
IPSec Pass Through	Ermöglicht die Nutzung von IP Security Pass Through.
PPTP Pass Through	Ermöglicht Ihnen die Anwendung eines PPTP (Point-to-Point Tunneling Protocol) zur Aktivierung von VPN Sessions.
Intrusion Detect	Diese Option erkennt Eingriffsversuche in Ihr Netzwerk und zeichnet sie auf.

5.3.1.6. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.3.2. Löschen von Filtern:

Sie können jeden bestehenden Port-Filter oder Raw IP-Filter löschen. Stellen Sie jedoch sicher, dass Sie nur unerwünschte Filter löschen; andernfalls kann das Löschen von zu virtuellen Servern oder speziellen Anwendungen dazugehörigen Filtern zum Ausfall von Diensten führen.

5.3.2.1. Löschen eines Port-Filters:

5.3.2.1.1. Geben Sie auf der Seite 'Filter' für jeden zu löschenden Port-Filter in den Feldern des 'Private Port Range' *0* ein.

5.3.2.1.2. Klicken Sie auf 'Apply'.

5.3.2.2. Löschen eines Raw IP-Filters:

5.3.2.2.1. Geben Sie auf der Seite 'Filter' für jeden zu löschenden Raw IP-Filter in dem Feld 'Proto Num' *0* ein.

5.3.2.2.2. Klicken Sie auf 'Apply'.

5.4 IP/URL Block

Auf der Seite 'IP/URL Block' können Sie Filter erstellen, die selektiv Benutzern bestimmter IP-Adressen oder Domainnamen den Zugang zu Ihrem Netzwerk verwehren. Der Unternehmens-AP-Router stellt zwei Arten zum Sperren von Benutzern zur Verfügung:

- **IP Block:** Ermöglicht das Sperren einzelner IP-Adressen oder einen Bereich von IP-Adressen.
- **URL Block:** Ermöglicht das Sperren von bis zu 36 Domainnamen.

Hinweis - Diese IP/URL Block-Funktion sperrt bestimmte IP-Adressen oder Domainnamen in beiden Richtungen.

Was möchten Sie tun?

- Sperren einer einzelnen IP-Adresse
- Sperren eines Bereiches von IP-Adressen
- Sperren eines bestimmten Domainnamens
- Löschen eines bestimmten oder aller IP Blocks
- Löschen eines bestimmten oder aller URL Blocks

5.4.1. Sperren einer einzelnen IP-Adresse:

Wählen Sie eine der folgenden Möglichkeiten:

5.4.1.1. Klicken Sie auf 'IP/URL Block' in der Navigationsleiste 'Advanced'.

5.4.1.2. Wenn Sie sich auf der Seite 'URL Block' befinden, wählen Sie 'IP Block' oben auf der Seite.

Die Seite 'IP Block' erscheint, siehe ABBILDUNG 5-6:

ABBILDUNG 5-6: Seite 'IP Block'

- 5.4.1.3. Geben Sie in den Zeilen 1 bis 6 in den Feldern der IP Block-Startadressen und denen der IP Block-Endadressen jeweils die gleichen IP-Adressen ein.
- 5.4.1.4. Optional: Sie können durch Klicken auf 'Clear All' ganz bequem alle bestehenden IP-Adressen löschen und dann mit Schritt 2 fortfahren.
- 5.4.1.5. Wenn Sie die Bearbeitung aller zu sperrenden IP-Adressen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.4.2. Sperren eines Bereiches von IP-Adressen:

- 5.4.2.1. Wählen Sie eine der folgenden Möglichkeiten:

Klicken Sie auf 'IP/URL Block' in der Navigationsleiste 'Advanced'.

Wenn Sie sich auf der Seite 'URL Block' befinden, wählen Sie 'IP Block' oben auf der Seite.

Die Seite 'IP Block' erscheint, siehe ABBILDUNG 4-6.

- 5.4.2.2. Geben Sie in den Zeilen 1 bis 6 in den Feldern der IP Block-Startadressen und denen der IP Block-Endadressen jeweils die verschiedenen IP-Adressen ein.
- 5.4.2.3. Optional: Sie können durch Klicken auf 'Clear All' ganz bequem alle bestehenden IP-Adressen löschen und dann mit Schritt 2 fortfahren.
- 5.4.2.4. Wenn Sie die Bearbeitung aller zu sperrenden IP-Adressen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

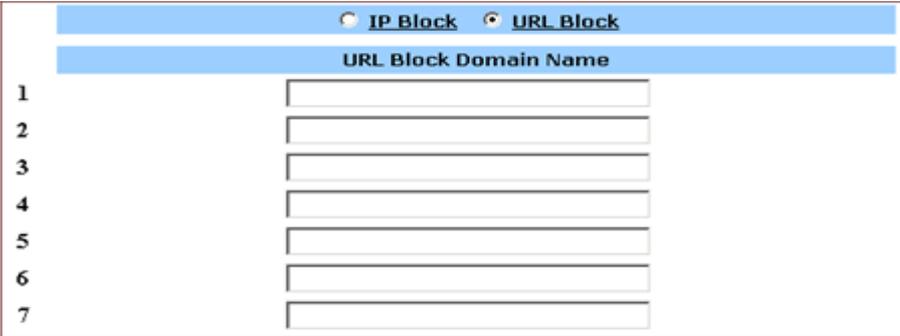
5.4.3. Sperren eines bestimmten Domainnamens:

5.4.3.1. Klicken Sie auf 'IP/URL Block' in der Navigationsleiste 'Advanced'.

Die Seite 'IP Block' erscheint, siehe ABBILDUNG 5-6.

5.4.3.2. Wählen Sie 'URL Block' auf der Seite 'IP Block'.

Die Seite 'URL Block' erscheint, siehe ABBILDUNG 5-7:



URL Block Domain Name	
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>

ABBILDUNG 5-7: Seite 'URL Block'

5.4.3.3. Geben Sie in die Zeilen 1 bis 36 die URLs ein, die Sie sperren möchten.

5.4.3.4. Optional: Sie können durch Klicken auf 'Clear All' ganz bequem alle bestehenden URLs löschen und dann mit Schritt 2 fortfahren.

5.4.3.5. Wenn Sie die Bearbeitung aller zu sperrenden Domainnamen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.4.4. Löschen eines bestimmten oder aller IP Blocks:

5.4.4.1. Wählen Sie auf der Seite 'IP Block' eine der folgenden Optionen:

Geben Sie für jeden IP Block, den Sie löschen wollen, sowohl in der IP Block-Startadresse als auch in der IP Block-Endadresse jeweils 0.0.0.0 ein. Wenn Sie alle IP Blocks löschen wollen, klicken Sie einfach 'Clear All'.

5.4.4.2. Klicken Sie auf 'Apply'.

5.4.5. Löschen eines bestimmten oder aller URL Blocks:

5.4.5.1. Wählen Sie auf der Seite 'URL Block' eine der folgenden Optionen:

Entfernen Sie in den Feldern alle URLs der Domainnamen, die Sie löschen wollen.

Wenn Sie alle URL Blocks löschen wollen, klicken Sie einfach 'Clear All'.

5.4.5.2. Klicken Sie auf 'Apply'.

5.5 Spezielle Anwendungen

Auf der Seite 'Special Apps' können Sie bestimmte Ports autorisieren, mit PCs außerhalb Ihres Netzwerks zu kommunizieren. Dies könnte für Multisession-Anwendungen wie Online-Spiele oder Sprachkonferenzen notwendig sein.

Es gibt zwei Arten, neue spezielle Anwendungen auf Ihrem Router einzurichten:

- **Popular Application Copy:** Ermöglicht die Auswahl einer von häufig genutzten Anwendungen aus der Dropdown-Liste 'Popular Applications' und das Kopieren in Ihre 'Special Applications'-Tabelle. Mögliche Optionen sind *AIM, Diablo II (1), Diablo II (2), StarCraft, StarCraft III, ICUII, FTP, CUseeMe, MSN Messenger* und *Real Player*.
- **Manuelle Konfiguration:** Wenn sich die Anwendungen, die Sie konfigurieren möchten, nicht in der 'Popular Applications'-Liste befinden, können Sie deren Einstellungen auch manuell konfigurieren.

Prüfen Sie vor dem Konfigurieren einer neuen speziellen Anwendung bitte zuerst die Liste der 'Popular Applications'. Falls sich die Anwendung bereits in der Liste befindet, empfehlen wir Ihnen, solange die 'Popular Application Copy'-Funktion anzuwenden, bis Sie genau wissen, welche Einstellungen

Hinweise:

Das Konfigurieren spezieller Anwendungen kann zum automatischen Erstellen von Filtern auf der Seite 'Filter' führen.

Der Unternehmens-AP-Router verfügt über zwei voreingestellte Spezialanwendungen für FTP und NetMeeting; das Überschreiben dieser oder anderer bestehenden Anwendungen führt zu deren Ausfall.

vorzunehmen sind.

Was möchten Sie tun?

- **Kopieren einer 'Popular Application' in eine bestimmte Zeile**
- **Manuelles Konfigurieren einer 'Special Application'**
- **Löschen einer speziellen Anwendung**

5.5.1. Kopieren einer 'Popular Application' in eine bestimmte Zeile:

5.5.1.1. Klicken Sie auf 'Special Apps' in der Navigationsleiste 'Advanced'.

Die 'Popular Applications'-Liste erscheint auf der Seite der 'Special Apps', siehe ABBILDUNG 5-8:

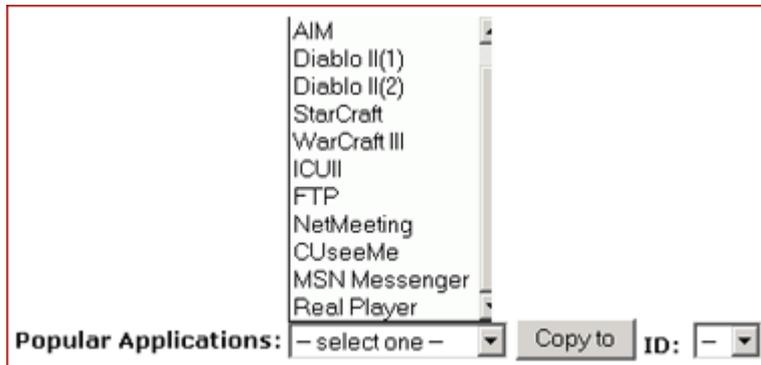


ABBILDUNG 5-8: 'Popular Applications'-Liste

5.5.1.2. Wählen Sie eine Option aus der 'Popular Applications'-Dropdown-Liste, die AIM, Diablo II (1), Diablo II (2), StarCraft, StarCraft III, ICUII, FTP, CUseeMe, MSN Messenger und Real Player enthält.

Hinweis:

Stellen Sie sicher, dass Sie die bestimmte ID in eine leere Zeile einfügen; es sei denn, Sie möchten eine bestehende Anwendung überschreiben.

Wählen Sie eine bestimmte Zeilennummer aus der 'ID'-Dropdown-Liste.

5.5.1.3. Klicken Sie auf 'Copy to'.

5.5.1.4. Die gewählte Konfiguration der Anwendung wird zu Ihrer 'Special Applications'-Tabelle oben auf der Seite hinzugefügt.

5.5.1.5. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.5.2. Manuelles Konfigurieren einer 'Special Application':

5.5.2.1. Klicken Sie auf 'Special Apps' in der Navigationsleiste 'Advanced'.

5.5.2.2. Die Seite 'Special Apps' erscheint, siehe ABBILDUNG 5-9:

ID	Protocol	Trigger Port Range	Maximum Activity Interval	Session Chaining	Chaining on UDP	Address Replacement	Address Translation Type	Two Way Only
1	TCP	21 - 21	3000	Disable	Disable	Disable	TCP	Enable
2	TCP	1720 - 1720	30000	Enable	Disable	Enable	TCP	Disable
3	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
4	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
5	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
6	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
7	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
8	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
9	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
10	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
11	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
12	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable

Apply Cancel Help

ABBILDUNG 5-9: Seite 'Special Apps'

5.5.2.3. Wählen Sie eine Zeile, die einer bestimmten ID entspricht.

Hinweis :

Vergewissern Sie sich, dass Sie eine leere Zeile ausgewählt haben; es sei denn, Sie beabsichtigen, eine bestehende Anwendung zu überschreiben.

Geben Sie die folgenden Informationen zur Konfiguration ein:

Größe	Beschreibung
Protocol	Bestimmt das Kommunikationsprotokoll, das von der Anwendung benutzt wird. Mögliche Optionen sind <i>TCP</i> , <i>UDP</i> und <i>Both</i> .
Trigger Port Range	Bereich der Ports, die für den ausgehenden Verkehr genutzt werden. Es wird das Gateway angesteuert, um bestimmte eingehende Anfragen zuzulassen.
Maximum Activity Interval	Maximale Anzahl von Millisekunden nach der 'Port Trigger'-Funktion, innerhalb derer eingehende Anfragen zugelassen werden.
Session Chaining	Ermöglicht Ihnen die Auswahl von Enable oder Disable. Dieses Feld bestimmt, ob dynamische Sessions verknüpft werden können, um so

	Multisession Triggering zuzulassen.
Chaining on UDP	Ermöglicht die Auswahl von Enable oder Disable, sofern 'Session Chaining' aktiviert wurde. Diese Option bestimmt, ob 'Session Chaining' im UDP zugelassen wird.
Address Replacement	Ermöglicht die Auswahl von Enable oder Disable, sofern 'Chaining on UDP' aktiviert wurde. Bestimmen Sie hier, ob eine binäre Adressenerneuerung durchgeführt werden sollte.
Address Translation Type	Ermöglicht Ihnen, zwischen TCP oder UDP zu wählen, sofern 'Address Replacement' aktiviert wurde. Legt fest, ob 'Address Translation' an TCP- oder UDP-Paketen durchgeführt wird.
Two Way Only	Ermöglicht Ihnen die Auswahl von Enable oder Disable. Dieses Feld bestimmt, ob eine neue Session durch den gleichen Remote Host eingeleitet werden darf.

5.5.2.4. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.5.3. Löschen einer speziellen Anwendung:

5.5.3.1. Geben Sie auf der Seite der 'Special Apps' für jede Anwendung, die Sie löschen möchten, 0 – 0 im Feld 'Trigger Port Range' ein.

5.5.3.2. Klicken Sie auf 'Apply'.

5.6 DMZ Host

Auf der Seite 'DMZ Host' können Sie einen oder mehrere Client-PCs Ihres Netzwerks für das Internet freigeben. Dies wird häufig für Online-Spiele genutzt, die unbeschränkte Kommunikation in beiden Richtungen erfordern.

Die Gesamtanzahl der DMZ (Demilitarized Zone) Hosts, die Sie haben können, ist abhängig von der Anzahl der Globalen Adressen, die Sie auf der Seite 'Global Address' konfiguriert haben. Sie haben zum Beispiel fünf Globale Adressen (inklusive der Standard-IP) definiert; dann ist auch die Anzahl der DMZ Hosts auf fünf begrenzt. Liegt die maximale Anzahl der Globalen Adressen bei

Vorsicht:

Nachdem ein PC in Ihrem Netzwerk als DMZ Host bestimmt wurde, verfügt er über keinerlei Firewall.

acht, können Sie auch bis zu acht DMZ Hosts konfigurieren.

Was möchten Sie tun?

- Einen PC in Ihrem Netzwerk zum DMZ Host bestimmen
- Löschen von DMZ Hosts

5.6.1. Einen PC in Ihrem Netzwerk zum DMZ Host bestimmen:

5.6.1.1. Klicken Sie auf 'DMZ Host' in der Navigationsleiste 'Advanced'.

Die Seite 'DMZ Host' erscheint, siehe ABBILDUNG 5-10:

Public IP Address	Private IP Address
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0

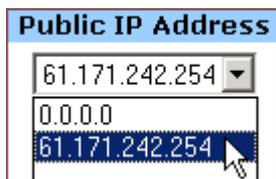
Apply Cancel Help

ABBILDUNG 5-10: Seite 'DMZ Host'

- 5.6.1.2. Wählen Sie eine 'Public IP Address' aus der Dropdown-Liste.
- 5.6.1.3. Geben Sie die IP-Adresse des PCs aus Ihrem Netzwerk, den Sie zum DMZ Host bestimmen wollen, in das 'Private IP Address'-Feld ein.
- 5.6.1.4. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.6.2. Löschen von DMZ Hosts:

- 5.6.2.1. Wählen Sie auf der Seite 'DMZ Host' für jeden DMZ Host, den Sie entfernen möchten, *0.0.0.0* aus der 'Public IP Address'-Dropdown-Liste.



- 5.6.2.2. Klicken Sie auf 'Apply'.

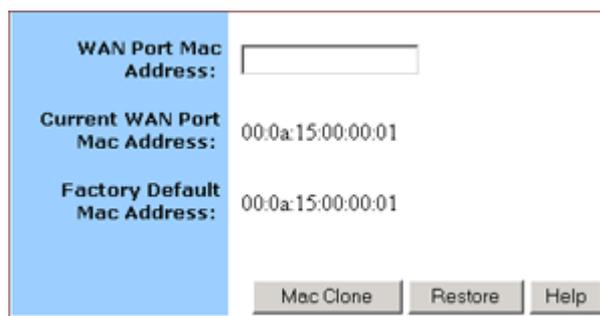
5.7 MAC Clone

Falls Ihr ISP Dienste auf PC-Ebene einschränkt, können Sie durch Anwendung von 'MAC Clone' eine PC MAC- (Media Access Control) Adresse auf den Router übertragen. Was wird dadurch passieren? Der Router erscheint als einzelner PC und mehrere PCs in Ihrem Netzwerk haben über diesen "Einzel-PC" Zugriff auf das Internet.

5.7.1. Klonen der MAC-Adresse:

5.7.1.1. Klicken Sie auf 'MAC Clone' in der Navigationsleiste 'Advanced'.

Die Seite 'MAC Clone' erscheint mit der aktuellen WAN Port-Adresse und der voreingestellten MAC-Adresse zu Ihrer Information, siehe ABBILDUNG 5-11:



WAN Port Mac Address:	<input type="text"/>
Current WAN Port Mac Address:	00:0a:15:00:00:01
Factory Default Mac Address:	00:0a:15:00:00:01
<input type="button" value="Mac Clone"/> <input type="button" value="Restore"/> <input type="button" value="Help"/>	

ABBILDUNG 5-11: Seite 'MAC Clone'

Hinweis:

Sie müssen eventuell die Ethernet MAC-Adresse der NIC (Network Interface Card) benutzen, mit der Ihr PC bei Ihrem ISP registriert ist.

5.7.1.2. Klicken Sie auf 'MAC Clone' oder 'Restore', um die Standardeinstellungen wiederherzustellen.

5.8 Dynamic DNS

Auf der Seite 'Dynamic DNS' können Sie Ihren Domainnamen mit einem dynamischen DNS-Provider verknüpfen. Diese Provider ermöglichen die Verknüpfung eines statischen Hostnamens mit einer dynamischen IP-Adresse; Sie können dann mit einer dynamischen IP-Adresse ins Internet gehen und Anwendungen benutzen, die eine statische IP-Adresse erfordern.

Der Unternehmens-AP-Router unterstützt drei dynamische DNS-Provider:

- DynDNS.org
- no-IP.com
- no-IP.com

Was möchten Sie tun?

- [Konfigurieren eines dynamischen DNS-Servers](#)
- [Deaktivieren eines dynamischen DNS-Server](#)

5.8.1. Konfigurieren eines dynamischen DNS-Servers:

5.8.1.1. Klicken Sie auf 'Dynamic DNS' in der Navigationsleiste 'Advanced'.

Die Seite 'Dynamic Server' erscheint, siehe **ABBILDUNG 5-12**:



ABBILDUNG 5-12: Seite 'Dynamic DNS'

5.8.1.2. Wählen Sie 'Enable' neben 'Dynamic DNS'.

5.8.1.3. Wählen Sie zwischen *DynDNS.org*, *no-IP.com* oder *no-IP.com* aus der 'Dynamic DNS Provider'-Dropdown-Liste.

5.8.1.4. Geben Sie Ihren Domainnamen in das Feld ein.

5.8.1.5. Geben Sie Ihren Account oder Ihre E-Mail-Adresse ein.

5.8.1.6. Geben Sie auch Ihr Passwort oder Key in das entsprechende Feld ein.

5.8.1.7. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.8.2. Deaktivieren eines dynamischen DNS-Servers:

5.8.2.1. Wählen Sie auf der Seite 'Dynamic DNS' die Option 'Disable' neben 'Dynamic DNS'.

5.8.2.2. Klicken Sie auf 'Apply'.

5.9 Proxy DNS

Auf der Seite 'Proxy DNS' können Sie einem Domainnamen eine Server-IP-Adresse zuordnen. Als DNS-Server für interne und DMZ-Netzwerke ermöglicht er Ihnen, lokale Geräte ohne externen DNS-Server in Ihrem Netzwerk anzuschließen. Dies vereinfacht die Konfiguration und das Management Ihres Netzwerks.

Was möchten Sie tun?

- Einen Proxy DNS-Server konfigurieren
- Löschen eines bestimmten oder aller Proxy DNS-Server
- Proxy DNS auf Ihrem Router deaktivieren

5.9.1. Einen Proxy DNS-Server konfigurieren:

5.9.1.1. Klicken Sie in der 'Advanced'-Navigationsleiste auf 'Proxy DNS'.

Die Seite 'Proxy DNS' erscheint, siehe ABBILDUNG 5-13:

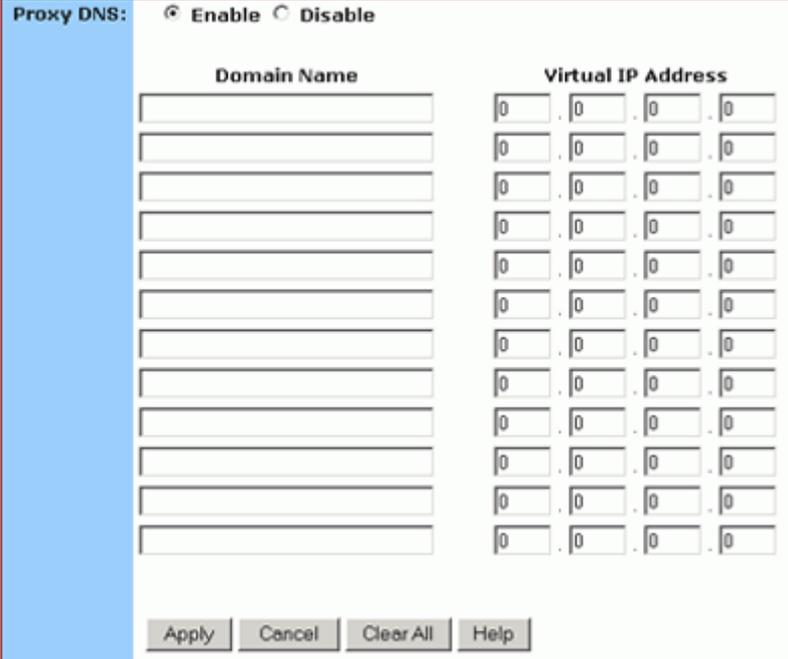


ABBILDUNG 5-13: Die Seite 'Proxy DNS'

5.9.1.2. Wählen Sie 'Enable' neben 'Proxy DNS'.

- 5.9.1.3.** Geben Sie in das Feld 'Domain Name' einen Namen für einen PC in Ihrem Netzwerk ein, den Sie als Proxy DNS-Server verwenden möchten .
- 5.9.1.4.** Geben Sie die IP-Adresse für den PC in das Feld 'Virtual IP Address' ein.
- 5.9.1.5.** Optional: Wenn Sie alle bestehenden Proxy DNS-Server zuerst löschen wollen, klicken Sie auf 'Clear All' und befolgen Sie die Schritte 3 und 4.
- 5.9.1.6.** Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.9.2. Löschen eines bestimmten oder aller Proxy DNS-Server:

- 5.9.2.1.** Geben Sie auf der Seite 'Proxy DNS' für den zu löschenden Proxy DNS-Server *0.0.0.0* in das Feld 'Virtual IP Address' ein.

Virtual IP Address						
0	.	0	.	0	.	0

- 5.9.2.2.** Wenn Sie alle bestehenden Proxy DNS-Server löschen möchten, klicken Sie auf 'Clear All'.
- 5.9.2.3.** Klicken Sie auf 'Apply'.

5.9.3. Proxy DNS auf Ihrem Router deaktivieren:

- 5.9.3.1.** Geben Sie auf der Seite 'Proxy DNS' für den zu löschenden Proxy DNS-Server *0.0.0.0* in das Feld 'Virtual IP Address' ein.

Virtual IP Address						
0	.	0	.	0	.	0

- 5.9.3.2.** Wenn Sie alle bestehenden Proxy DNS-Server löschen möchten, klicken Sie auf 'Clear All'.
- 5.9.3.3.** Klicken Sie auf 'Apply'.

5.10 SNMP

Das Simple Network Management Protocol (SNMP) ist ein Application Layer Protocol, das den Austausch von Managementinformationen zwischen Netzwerkgeräten ermöglicht. Es ist Teil des TCP/IP- (Transmission Control protocol/Internet Protocol) Satzes und ermöglicht Ihnen die Kontrolle und Überwachung des Netzwerks auf einfache Art.

Auf der Seite 'SNMP' können Sie die grundlegenden Agent-Informationen bearbeiten und außerdem bis zu 6 SNMP Trap Receiver IP-Adressen konfigurieren. Wenn ein Trap-Zustand auftritt, sendet Ihr Router eine SNMP Trap-Meldung an irgendein NMS (Network Management System), das als Trap Receiver angegeben ist, zum Beispiel, wenn Fehler in der

Hinweise:

Das NMS (Network Management System) ist eine SNMP-Managementanwendung und schließt den Computer, auf dem sie läuft, mit ein.

Gegenwärtig unterstützt der Unternehmens-AP-Router SNMPv1 (SNMP version 1) und SNMPv2 (SNMP version 2), die außer einigen Verbesserungen eine Reihe von Funktionen gemeinsam haben.

Spannungsversorgung auftreten.

Zusätzlich können Sie verschiedene Community-Namen für die Authentifizierung des Zugangs zur Managementinformation festlegen, die als eingebettete Passwörter funktionieren:

- 'Read': Gibt Ihnen LESE-Zugriff auf alle Managementinformationen, erlaubt aber den SCHREIB-Zugriff nicht.
- 'Write': Gibt Ihnen LESE- und SCHREIB-Zugriff auf alle Managementinformationen.

Hinweis:

Der Community Namensdefinitionen auf Ihrem NMS müssen mit mindestens einer der oben stehenden zwei Community-Namensdefinitionen übereinstimmen.

Was möchten Sie tun?

- Agent-Informationen, SNMP Trap Host IP-Adressen und Community-Namen auf Ihrem Router konfigurieren
- Löschen eines bestehenden SNMP Trap-Receiver
- Löschen von SNMP Community-Namen

5.10.1. Agent-Informationen, SNMP Trap Host IP-Adressen und Community-Namen auf Ihrem Router konfigurieren:

5.10.1.1. Klicken Sie in der 'Advanced'-Navigationsleiste auf 'SNMP'.

Die Seite 'SNMP' erscheint, siehe ABBILDUNG 5-14:

The screenshot shows the SNMP configuration interface. On the left, a blue sidebar contains labels for 'Name:', 'Contact:', 'Location:', and six 'SNMP Trap Host IP' fields. The main content area has input fields for 'Name' (containing 'SOHO Router'), 'Contact', and 'Location'. Below these are six rows of IP address input fields, each consisting of four boxes separated by dots. At the bottom of the main area are 'Apply', 'Cancel', and 'Help' buttons. Below the main area is a 'Community List' table with columns for 'SNMP Community', 'SNMP Access', and actions. The table has one row with ID 1, Community 'None', and Access 'None'.

ABBILDUNG 5-14: Die Seite 'SNMP'

Geben Sie die folgenden Agent-Informationen ein:

Größe	Beschreibung
Name	<p>Bestimmt einen administrativ zugewiesenen Namen für diesen gemanagten Knoten, wie z.B. <i>SOHO Router</i>.</p> <p>Dies ist eine Zeichefolgen mit höchstens 31 alphanumerischen Zeichen.</p>
Contact	<p>Legt die Kontaktperson dieses gemanagten Knotens fest, einschließlich Telefonnummer, Email-Adresse, etc.</p> <p>Dies ist eine Zeichefolgen mit höchstens 255 alphanumerischen Zeichen.</p>
befindet sich	<p>Legt die physische Lage dieses gemanagten Knotens fest, zum Beispiel, Stadt, Adresse und Bürolage.</p> <p>Dies ist eine Zeichefolgen mit höchstens 255 alphanumerischen Zeichen.</p>

5.10.1.2. Um SNMP Trap-Meldungen an irgendein NMS zu senden, geben Sie bis zu 6 Trap Receiver IP-Adressen in die Felder 'SNMP Trap Host IP Address 1' – 'SNMP Trap Host IP Address 6' ein.

5.10.1.3. Um SNMP mit Community-Namen zu sichern, tun Sie das Folgende:

5.10.1.3.1. Geben Sie eine Zeichefolge in das Feld 'SNMP Community' ein.

5.10.1.3.2. Wählen Sie eine Option aus der Dropdown-Liste 'SNM Access', zum Beispiel 'Read'.

Note :

Usually, we define a string of “Public” for Read access and “Private” for Read-Write access.

5.10.1.3.3. Klicken Sie auf 'Add'. Wenn Sie mehrere Community-Namen hinzufügen möchten, wiederholen Sie bitte die Schritte 4.1 – 4.3.

5.10.1.4. Wenn Sie die Bearbeitung Ihrer Einstellungen abgeschlossen haben, klicken Sie auf 'Apply'; wenn Sie Ihre Änderungen zurücksetzen möchten, klicken Sie auf 'Cancel'.

5.10.2. Löschen eines bestehenden SNMP Trap-Receiver:

5.10.2.1. Geben Sie auf der Seite 'SNMP' für irgendeinen SNMP Trap Receiver, den Sie löschen möchten, *0.0.0.0* in das Feld 'SNMP Trap Host IP Address' ein.

Community List:			
	SNMP Community	SNMP Access	
	<input type="text"/>	Read	<< Add
1	Public	Read	Delete

5.10.2.2. Klicken Sie auf 'Apply'.

5.10.3. Löschen von SNMP Community-Namen:

5.10.3.1. Klicken Sie auf der Seite 'SNMP' für irgendeinen SNMP Community-Namen, den Sie löschen möchten, in der entsprechenden Zeile auf 'Delete'.

5.10.3.2. Klicken Sie auf 'Apply'.

5.11 Statisches Routing

Das Statische Routing wird verwendet, um statische Routes zu Remote-Netzwerken manuell zu konfigurieren, wo die Route vordefiniert ist und nicht durch das Routing Information Protocol (RIP) überwacht wird. Dies kann den Netzwerkverkehr explizit reduzieren und die Internetverbindungen für ein kleines Netzwerk beschleunigen.

Jedoch können bestimmte Nachteile auftreten. Wenn ein statischer Router mehr als einen Hop einbezieht, wenn die Verbindung zum nächsten Hop abbricht, kann der Router den ungültigen Pfad nicht erkennen und routet den Verkehr weiter auf diesen Hop.

Auf der Seite 'Static Routing' können Sie bis zu 20 statische Routes hinzufügen, indem Sie Folgendes angeben:

- Ziel-LAN IP-Adresse und Subnet Mask
- Remote Gateway
- Hop
- Router-Schnittstelle, durch die die Pakete zum Ziel weitergeleitet werden.

Hinweis:

Wenn sich die Netzwerktopologie ändert, müssen Sie vielleicht Änderungen an den 'Static Routing Tables' für relevante statische Routes vornehmen.

Was möchten Sie tun?

- Neue statische Route hinzufügen
- Statische Route löschen

5.11.1. Neue statische Route hinzufügen:

5.11.1.1. Klicken Sie in der 'Advanced'-Navigationsleiste auf 'Routing'.

Die Seite 'Static Routing' erscheint, siehe ABBILDUNG 5-15:

Static Routing:												
Destination LAN IP				Subnet Mask				Gateway		Hop	Interface	
<input type="text"/>	WAN	<< Add										
192.168.99.10				255.255.255.0				192.168.99.1		3	WAN	Delete

ABBILDUNG 5-15: Die Seite 'Static Routing'

5.11.1.2. Geben Sie die folgenden Static Route-Informationen ein:

Größe	Beschreibung
Destinati on LAN IP	Gibt die Netzwerk-Adresse des Remote LAN-Segments an. Für Standard-Klasse-"C"-LANs ist die Netzwerkadresse die ersten 3 Felder dieser Ziel--LAN IP, das 4. Feld kann auf 0 gelassen werden.
Subnet Mask	Gibt die Subent-Mask an, die auf dem Remote LAN Segment verwendet wird. Für Klasse-"C"-Netzwerke ist die Standard Network Mask 255.255.255.0.
Gateway	Gibt die IP-Adresse des Routers auf dem lokalen LAN-Segment an, an das das Gerät angebunden ist. Beachten Sie, dass dies NICHT der Router auf dem Remote LAN-Segment ist.
Hop	Gibt die Anzahl der Router auf dem Weg zum Remote LAN-Segment an. Gültig sind Werte von 1 bis 16.
Schnittste lle	Gibt die Schnittstelle an, durch die der Router zum nächsten Hop oder zu einem bestimmten Netzwerk geht. Verfügbare Optionen sind WAN, LAN und DMZ.

5.11.1.3. Klicken Sie auf <<'Add'.

Die neue statische Route wird in der 'Static Routing'-Liste angezeigt.

5.11.2. Statische Route löschen:

5.11.2.1. Beachten Sie auf der Seite 'Static Routing' für jede statische Route, die Sie löschen möchten, die relevanten Informationen, siehe ABBILDUNG 5 – 15.

5.11.2.2. Klicken Sie auf 'Delete'.

6. Glossar

IEEE 802.11 Standard

Das IEEE-Subkomitee für Wireless LANs hat den Standard 802.11 für die gesamte Branche formuliert.

Access Point

Ein Netzwerkgerät, das eine nahtlose Verbindung zwischen verkabelten und Wireless-Netzwerken erstellt.

Ad hoc

Ein Ad-hoc-Wireless LAN ist eine Gruppe von mit WLAN-Adaptoren ausgestatteten Computern, die zu einem unabhängigen Wireless LAN verbunden sind. Ad-hoc-Wireless LAN ist geeignet für den Gebrauch in Abteilungen, Zweigstellen oder den SOHO-Betrieb.

BSSID

Ein bestimmtes Ad-hoc-LAN wird Basic Service Set (BSS) genannt. Auf allen Computern in einem BSS muss die gleiche BSSID konfiguriert sein.

DHCP

Dynamic Host Configuration Protocol - ein Verfahren zur dynamischen Vergabe von IP-Adressen durch den Server an Netzwerkteilnehmer. DHCP wird zur dynamischen Vergabe von IP-Adressen verwendet und benötigt einen DHCP-Server im Netzwerk, dem diese Aufgabe zugewiesen ist.

DSSS

Direct Sequence Spread Spectrum. Diese Methode verwendet drahtlose Adapter, um Daten über das Frequenzspektrum zu übertragen. Ein alternatives Verfahren heißt Frequency Hopping. Beim Direct-Sequence-Verfahren werden die Daten über einen Frequenzbereich (Kanal) verteilt, während beim Frequency Hopping mehrere Male in der Sekunde von einem schmalen Frequenzband zum anderen gesprungen wird.

ESSID

Eine Infrastruktur-Konfiguration, die auch mobilen Internetzugang für mobile Mitarbeiter unterstützen kann. Mehr als ein BSS kann als Extended Service Set (ESS) konfiguriert werden. Benutzer innerhalb des ESS können sich frei zwischen den BSSs bewegen, während Verbindung zu den Stationen des Wireless-Netzwerks besteht. Access Points innerhalb des ESS müssen über die gleiche BSSID und den gleichen Funkkanal konfiguriert sein.

Ethernet

Ethernet ist ein 10/100-Mbps-Netzwerk, das auf eigenen Heim- oder Büroleitungen läuft. Die Benutzer müssen immer mit dem Netzwerk verkabelt sein, um Zugang zu erhalten.

Gateway

Ein Gateway ist ein Gerät, das zwei verschiedene Systeme miteinander verbindet, zum Beispiel ein LAN und einen Mainframe. In der Internet-Terminologie ist Gateway ein anderer Name für Router. Normalerweise dient ein Gateway als eine Art Trichter für den gesamten Verkehr zum Internet.

IEEE

Institute of Electrical and Electronics Engineers

Infrastructure

Integrierte Wireless- und verkabelte LANs werden als Infrastruktur-Konfigurationen bezeichnet. Infrastruktur wird auf Unternehmensebene für drahtlosen Zugang zur zentralen Datenbank oder für die drahtlose Anbindung mobiler Mitarbeiter verwendet.

ISM-Band

Die FCC und verwandte Organisationen außerhalb der USA haben einen Frequenzbereich festgelegt, der lizenzfrei für industrielle, wissenschaftliche und medizinische Anwendungen (ISM, Industrial, Scientific, Medical) genutzt werden darf. Das Spektrum liegt weltweit im Bereich um 2,4 GHz. Dies bietet die wahrhaft revolutionäre Gelegenheit, bequeme High-Speed-Wireless-Anwendungen für Benutzer in der ganzen Welt anzubieten.

LAN

Local Area Network. Ein LAN besteht aus einer Gruppe von Rechnern, die alle mit einem geeigneten Netzwerkadapter ausgestattet sind, über Kabel oder Funk vernetzt sind und sich Anwendungen, Daten und Peripheriegeräte teilen. Verbindungen verlaufen über Kabel oder Wireless-Medien. LANs nutzen keine Telefonleitungen. Ein LAN umspannt normalerweise ein einzelnes Gebäude oder einen Campus.

Netzwerk

Ein Netzwerk ist ein System von verbundenen Computern. Daten, Dateien und Nachrichten können auf diesem Netzwerk übertragen werden. Netzwerke können lokal (LAN, Local Area Network) sein oder ein größeres Gebiet umschließen (WAN, Wide Area Network).

Protocol

Ein Protokoll ist ein standardisierter Satz von Regeln, der bestimmt, wie Daten übertragen werden, einschließlich Format, zeitlichem Ablauf, Sequenzierung und/oder Fehlerprüfung.

SSID

Service Set Identifier. Eine Netzwerk-Kennung, die eindeutig für jedes Netzwerk ist. Nur Clients und Access Points, die sich die selbe SSID teilen, können miteinander kommunizieren. Bei dieser Zeichenfolge ist auf Groß- und Kleinschreibung zu achten.

SNMP

Simple Network Management Protocol ist das Netzwerk-Managementprotokoll von TCP/IP. Im SNMP überwachen Hardware- oder Software-Agenten die Aktivitäten der verschiedenen Geräte im Netzwerk und liefern Berichte an die Netzwerk-Konsolen-Workstation. Steuerungsinformationen über jedes Gerät werden in einer Struktur namens Management Information Block verwaltet.

Statische IP-Adressierung

Ein Verfahren, um Clients im Netzwerk IP-Adressen zuzuweisen. Bei Netzwerken mit statischer IP-Adressierung weist der Netzwerkadministrator jedem Computer eine IP-Adresse zu. Nachdem eine statische IP-Adresse zugewiesen wurde, verwendet der Computer bei jedem Start und jeder Anmeldung die gleiche IP-Adresse, es sei denn, sie wird manuell geändert.

TCP/IP

Transmission Control Protocol / Internet Protocol. TCP/IP ist eine Reihe von Protokollen, die von der Advanced Research Projects Agency (ARPA) entwickelt wurde. TCP bestimmt, wie Pakete für eine Übertragung im Netzwerk sequenziert werden. Der Begriff "TCP/IP" wird häufig verwendet, um auf den gesamten Satz von verwandten Protokollen zu verweisen.

Transmit/Receive (Senden/Empfangen)

Der Durchsatz einer Wireless-Verbindung in Bytes pro Sekunde (Bps). Er wird immer über zwei Sekunden ermittelt.

WAN

Wide Area Network. Ein WAN besteht aus mehreren LANs, die durch Telefonleitungen und/oder Glasfaserleitungen miteinander verbunden sind. WANs können sich über eine Stadt, einen Staat, ein Land oder sogar über die ganze Welt erstrecken.

acer
we hear you

<http://www.acer-euro.com>