



FRITZ!Box 3270

Installation,
Configuration
and Operation



Table of Contents

	Symbols and Highlighting	6
1	Getting to Know Your FRITZ!Box	7
1.1	The FRITZ!Box at a Glance	7
1.2	Ports and Interfaces	9
1.3	Buttons	10
1.4	LEDs	11
2	Before You Connect the FRITZ!Box	12
2.1	Contents of the FRITZ!Box Package	12
2.2	Requirements for Operation	12
2.3	Security and Handling	13
3	Connecting the FRITZ!Box	15
3.1	Connecting to Electrical Power	15
3.2	Connecting to the Internet	16
4	Connecting the Computer to the FRITZ!Box	17
4.1	Connecting Computers to the LAN Port	17
4.2	Connecting Computers Wirelessly over WLAN	19
5	The FRITZ!Box User Interface	25
5.1	Opening the User Interface	25
5.2	Protecting the User Interface with a Password	26
5.3	Saving the FRITZ!Box Settings	27
6	Configuring an Internet Connection in the FRITZ!Box ..	28
6.1	Configuring an Internet Connection for DSL	28
6.2	Changing the Annex Setting of the FRITZ!Box	29
6.3	Configuring the Internet Connection for Cable	30
6.4	Configuring the Internet Connection for the Mobile Telephone Network	30
6.5	Surfing the Net	31

7	Firmware Update: Updating the FRITZ!Box Software . .	32
8	The FRITZ!Box as an Internet Router	33
8.1	Child Protection: Restricting Internet Access	33
8.2	Port Forwarding: Making Computers Accessible from the Internet.	34
8.3	Dynamic DNS: Name Instead of IP Address	35
8.4	Remote Access over HTTPS	36
8.5	Prioritization: Right of Way for Internet Access	36
8.6	VPN: Remote Access to the Home Network	39
8.7	DNSSEC: Security for DNS Queries	41
8.8	IPv6: The New Internet Protocol	42
9	The FRITZ!Box as a WLAN Base Station	44
9.1	Security.	44
9.2	Guest Access: WLAN Connection for Guests	44
9.3	Setting Up Night Service for WLAN	45
9.4	Increasing the Range of the WLAN Connection	47
9.5	WLAN Standards	49
9.6	Frequency Ranges	54
10	The FRITZ!Box Home Network.	58
11	Network Devices in the FRITZ!Box Home Network . . .	60
11.1	Network Settings in the FRITZ!Box	60
11.2	Obtaining an IP Address Automatically	66
12	USB Devices in the FRITZ!Box Home Network.	71
12.1	Power Supply for USB Devices	71
12.2	USB Devices on the FRITZ!Box.	71
12.3	Using USB Devices Safely	72
12.4	Accessing USB Memory.	72
12.5	Sharing a USB Printer	73

13	Saving Energy with the FRITZ!Box	79
13.1	Saving Energy with the WLAN Radio Network	79
13.2	Enabling Energy-saving Mode for USB Hard Drives	79
13.3	Saving Energy at the LAN Ports	80
14	Help in Case of Errors	81
14.1	Cannot Establish a DSL Connection	81
14.2	The User Interface Does Not Open	82
14.3	Cannot Establish a WLAN Connection	88
15	Taking the FRITZ!Box out of Operation	94
15.1	Restoring the FRITZ!Box Factory Settings	94
15.2	Uninstalling Software	95
16	Technical Specifications	96
16.1	Ports and Interfaces	96
16.2	Router Functions	96
16.3	User Interface and Display	97
16.4	Physical Specifications	97
16.5	Cable	97
17	Customer Service	98
17.1	Documentation on the FRITZ!Box	98
17.2	Information in the Internet	98
17.3	Support from the Support Team	99
17.4	Manufacturer's Warranty	100
18	AVM Products for the FRITZ!Box	102
	Legal Notice	107
	Legal Notice	107
	Declaration of CE Conformity	108
	Disposal Information	109

Drilling Template.....	110
Glossary.....	112
Index	130

Symbols and Highlighting

Symbols and emphasized text are used to mark certain information in this manual.

Symbols



This symbol designates hints and tips that are useful in operating your product.



This symbol indicates important instructions that must be observed to avoid malfunctions.

Highlighting

Highlighting	Function	Examples
Quotation marks	Keys	“F1” key
	Buttons	“Help”
	Menus	“Home Network”
	File paths	“C:\My Documents”
	Folder and file names	“Info”
Pointed brackets	Joker	‹Telephone number›
Blue and underlined text	Address to be entered in the web browser	fritz.box
Blue text	Links and references within this manual	For more information on customer service, see the section from page 98 .
Bold text	Emphasis	Do not click the button ...

1 Getting to Know Your FRITZ!Box

This chapter gives you an overview of the features and functions of your FRITZ!Box 3270 and describes ports, buttons and LEDs.

1.1 The FRITZ!Box at a Glance

Access to the Internet

The FRITZ!Box connects multiple computers fast and safely with the Internet. Other network-compatible devices like smartphones and game consoles can use the FRITZ!Box for their Internet connection.

For fast Internet connections an ADSL modem is integrated into the FRITZ!Box. A preconfigured firewall protects your network from attacks from the Internet.

The FRITZ!Box also offers a variety of functions to control access to the Internet as well as access from the Internet. The “Internet filter” feature allows you to restrict access to the Internet for individual Windows users or computers, for instance for your children’s computers. With the integrated VPN server you can link remote computers securely with the home network of the FRITZ!Box over the Internet.

WLAN Base Station for Wireless Connections

Computers and other network devices that support WLAN can be connected wirelessly with the FRITZ!Box. If no WLAN device is integrated in your computer, you can install an external WLAN adapter like a FRITZ!WLAN USB Stick by AVM (see also [AVM Products for the FRITZ!Box from page 102](#)).

The FRITZ!Box supports the fast WLAN N standard, which provides for data throughput of up to 300 Mbit/s (gross).

You can use the FRITZ!Box in either the 2.4-GHz frequency band or the 5-GHz frequency band (dual band). Because the 5-GHz frequency band is used less frequently, connections in this band are subject to less interference.

With the “guest access” feature you can grant friends and visitors fast, secure access to the Internet over your wireless network.

Switchboard in the Home Network

The FRITZ!Box connects your computers and other network devices not only with the Internet, but also with each other. The connected network devices constitute the home network of the FRITZ!Box and can exchange data among each other.

You connect computers and other network devices with the FRITZ!Box either wirelessly via WLAN or using a network cable.

The FRITZ!Box can manage various storage media and make them available to all participants in the home network. These include connected USB flash drives, USB hard drives and on-line storage.

USB 2.0 Port

The FRITZ!Box has a USB port which can be used to integrate USB devices into your home network, for instance a printer or a storage medium. The connected USB devices can then be used simultaneously by all network devices in the home network of the FRITZ!Box.

If you connect a USB modem for mobile broadband Internet (UMTS/HSPA), the FRITZ!Box can establish Internet connections via the mobile communications network.

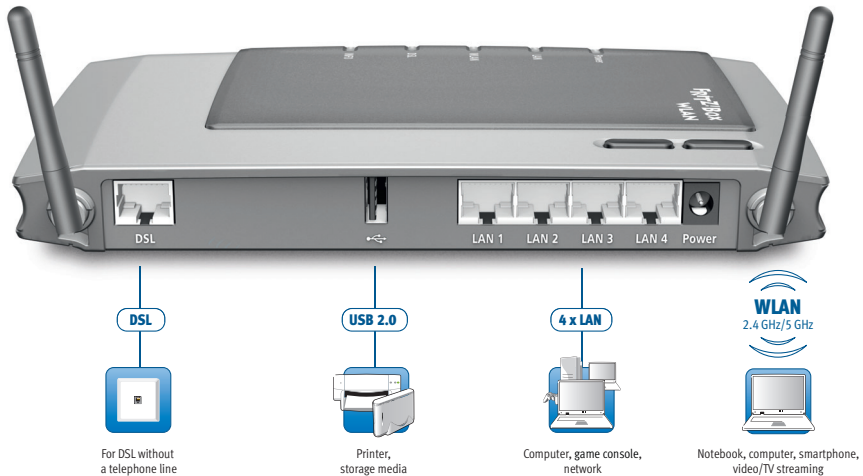
Media Server for Music, Images, and Video in the Home Network

As a media server the FRITZ!Box makes music, video and image files available throughout the entire home network. With suitable playback devices in the home network of the FRITZ!Box you can even play back the media files when the computer is turned off.

Your music, video and image files can be stored on a USB storage medium connected to the FRITZ!Box.

The playback devices or programs, for instance computers or television sets, must support the UPnP AV or DLNA standard.

1.2 Ports and Interfaces

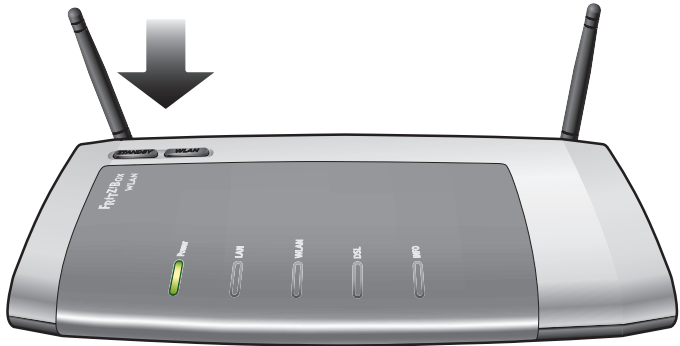


Possibilities for connecting the FRITZ!Box

- **DSL**
Socket for connecting to ADSL2+ ([see glossary](#)) and ADSL ([see glossary](#))
- **LAN 1 – LAN 4**
4 Ethernet ports (10/100 Base-T) for connecting computers and other network devices like game consoles and network hubs
- **USB** 
USB 2.0 port for connecting USB devices like printers or storage media
- **WLAN base station**
Integrated WLAN base station for connecting to WLAN devices that use the radio standard IEEE 802.11a, IEEE 802.11b, IEEE 802.11g or IEEE 802.11n (in the 2.4- or 5-GHz frequency band)

1.3 Buttons

The FRITZ!Box has two buttons on the upper side of the housing.



FRITZ!Box buttons

WLAN Button

With the “WLAN” button you can turn the WLAN function on and off and connect wireless devices with the FRITZ!Box by WPS. WPS is an easy way to establish secure wireless connections (see [page 20](#)).

STANDBY Button

The “STANDBY” button was originally included for the energy-saving mode. However, this function was never allocated to the button.

With the latest firmware the energy-saving mode is switched on and off automatically by the FRITZ!Box.

1.4 LEDs

Five LEDs are built into the top of the FRITZ!Box 3270, which flash or light up to display various connection statuses and events.

LED	Condition	Meaning
Power	on	• Device has electrical power and the DSL line is ready for operation
	flashing	• Device has electrical power and the connection to DSL is being established or has been interrupted
LAN	on	Network connection is active to at least one connected device (network adapter or hub/switch)
WLAN	on	WLAN function is enabled
	flashing	• Switching the WLAN function on or off • Adopting the WLAN settings • Performing WPS • WPS procedure aborted: More than two WLAN devices are performing WPS at the same time. Repeat the WPS procedure.
DSL	on	Internet connection active
Info	flashing	• Updating the firmware • Online meter reached the defined value, or another event defined in the user interface under “System / “Info” Display” is signaled
	flashing red	Error: Open the FRITZ!Box user interface and follow the instructions on the “Overview” page

2 Before You Connect the FRITZ!Box

- Check the contents of your FRITZ!Box package. See the section [Contents of the FRITZ!Box Package on page 12](#) for more information.
- Make sure that the requirements for connecting and operating the FRITZ!Box have been met. See the section [Requirements for Operation on page 12](#) for more information.
- Please see the security and handling instructions in the section [Security and Handling on page 13](#).

2.1 Contents of the FRITZ!Box Package

- FRITZ!Box 3270
- one power supply unit
- one network cable
- one DSL cable
- printed product information

2.2 Requirements for Operation

In order to operate the FRITZ!Box, you must have the following:

- a web browser that supports Java script (for instance, Internet Explorer version 8.0 or higher, or Firefox version 7 or higher)
- a connection to the Internet
 - a DSL line, standard ITU G.992.1 Annex A and B (G.dmt), ITU G.992.3 Annex A and B (ADSL2), ITU G.992.5 Annex A and B (ADSL2+), ITU G.992.3/5 Annex M, ITU G.992.3/5 Annex J, ITU G.994.1 (G.hs)
 - or an Internet cable access with cable modem
 - or a USB modem for mobile Internet access (UMTS /HSPA)
 - or another Internet connection

- for connecting computers via WLAN:
computer with WLAN support (compliant with IEEE 802.11n, IEEE 802.11g, IEEE 802.11a or IEEE 802.11b). Computers that do not have integrated WLAN can be equipped with WLAN support by installing a WLAN device like a FRITZ!WLAN USB Stick N, for instance.
- for connecting computers using network cable:
computer with a network port (network adapter standard Ethernet 10/100 Base-T)

2.3 Security and Handling

Before installing and using the FRITZ!Box, please read the following security and handling instructions.

Safety Instructions



When working with the FRITZ!Box 3270, be sure to observe the following security instructions in order to protect yourself and the FRITZ!Box from harm.

- Before mounting the FRITZ!Box on the wall, make sure that there are **no** electrical lines, gas or water pipes located where you need to drill the holes.
If necessary, check the site with a pipe detector or consult with qualified experts.
- Do not place FRITZ!Box on excessively heat-sensitive surfaces, as the base of the device can heat up during normal operation.
- Make sure that the ventilation slits on the FRITZ!Box housing are always unobstructed. The ventilation slits provide for air cooling.
 - The FRITZ!Box should not be placed on a carpet or on upholstered furniture.
 - Do not cover the FRITZ!Box.
- Do **not** install the FRITZ!Box during an electrical storm.

- Disconnect the FRITZ!Box from the power supply and from the DSL or VDSL line during electrical storms.
- Never let liquids get inside the FRITZ!Box. Otherwise, electric shocks or short circuits may result.
- The FRITZ!Box is intended for indoor use only.
- Do not open the FRITZ!Box housing. The device contains hazardous components and should only be opened by authorized repair technicians.

Handling the FRITZ!Box

- You can either place FRITZ!Box on a horizontal surface or mount it on a wall. For a drilling template to mount the FRITZ!Box on a wall, see [page 110](#).
- Place or hang the FRITZ!Box in a dry location that is free of dust and protected from direct sunlight.
- For ideal operating conditions, mount the FRITZ!Box on a wall with the cables connected on the bottom.
- When connecting FRITZ!Box to your computer using a network cable, keep in mind that the cable can be no longer than 100 m.
- If you would like to establish wireless connections between the FRITZ!Box and the computer, position the FRITZ!Box at a central location.
- Make sure to keep sufficient distance from potential sources of interference like microwave devices or electric devices with large metal housings.

3 Connecting the FRITZ!Box

- Connect the FRITZ!Box to the power supply.
- Connect the FRITZ!Box to your Internet connection.

This chapter tells you how.



Before you connect the FRITZ!Box, note the additional instructions in the section [Security and Handling on page 13](#).

3.1 Connecting to Electrical Power



Connecting to the power supply

1. Pick up the power supply unit included in the FRITZ!Box package.



Use only this power supply unit for connecting to electrical power.

2. Connect the power supply unit to the socket on the FRITZ!Box labeled “Power”.
3. Plug the other end into an AC power outlet.

The “Power” LED begins flashing after a few seconds to indicate that the FRITZ!Box is ready for operation.

3.2 Connecting to the Internet

Connect the FRITZ!Box to your Internet connection.

The FRITZ!Box can be connected using various types of Internet connections:

- DSL line
- Internet cable access using a cable modem
- Internet via mobile telephone network using a UMTS/HSPA modem

Connecting with a Cable Connection

With an additional cable modem you can also use your FRITZ!Box 3270 on a cable connection. Use a network cable.

1. Connect one end of the network cable to the LAN (Ethernet) port on the cable modem.
2. Connect the other end of the network cable to the socket on FRITZ!Box labeled “LAN 1”.
3. Connect a computer with the FRITZ!Box either wirelessly via WLAN or using a network cable (see [page 17](#)).
4. Set up the Internet connection for connections via cable in the FRITZ!Box (see [page 30](#)).

Connecting with the Internet via the Mobile Telephone Network

If no other kind of Internet connection is available, you can use your FRITZ!Box to connect to the Internet via the mobile telephone network. A USB modem for mobile Internet access (UMTS/HSPA) is required for this.



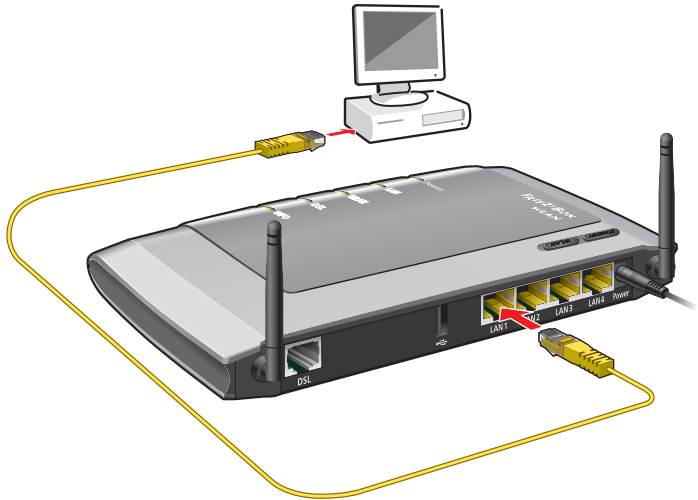
The FRITZ!Box supports UMTS/HSPA modems from various manufacturers.

1. Insert the USB modem into the USB port on the FRITZ!Box.
2. Set up the Internet connection via the mobile telephone network (see [page 30](#)).

4 Connecting the Computer to the FRITZ!Box

Connect one or several computers to the FRITZ!Box.

4.1 Connecting Computers to the LAN Port



Connecting a computer to a LAN port on the FRITZ!Box

1. Set aside the network cable (yellow) from the FRITZ!Box package.
2. If you work with a Linux operating system: Configure the network adapter of the computer with the setting “DHCP”.
3. Connect one end of the network cable to the network port (network card) of the computer.
4. Connect the other end to the “LAN 1”, “LAN 2”, “LAN 3” or “LAN 4” socket on the FRITZ!Box.

Now the FRITZ!Box and the computer are connected to each other.

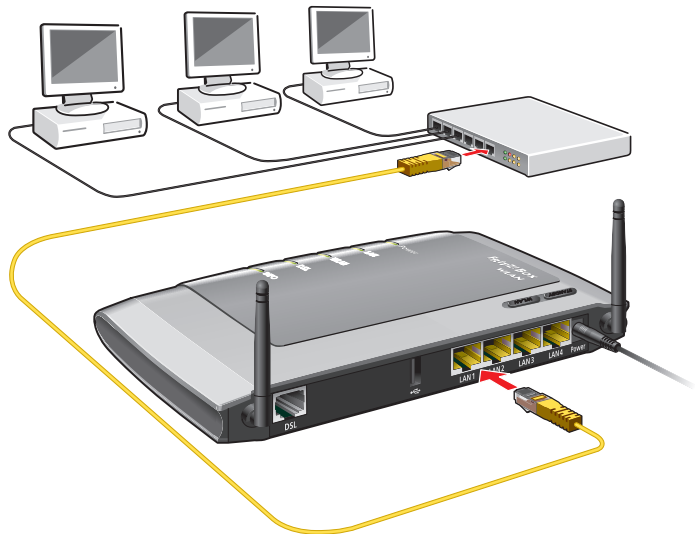
Connecting More Computers to the LAN Ports

Additional cables are required to connect further computers. In purchasing a LAN cable, note the instructions in the section [Network Cable on page 97](#).

One computer can be connected to each network port of the FRITZ!Box.

Connecting a Network Hub or Switch

You can also connect a network hub or switch to the LAN ports on the FRITZ!Box.



Connecting FRITZ!Box to a network hub

1. Set aside the network cable (yellow) from the FRITZ!Box package.
2. Connect one end of the LAN cable to the uplink port ([see glossary](#)) of the network hub or network switch.
3. Connect the other end of the cable to one of the LAN ports on the FRITZ!Box.

The FRITZ!Box and the network hub are now connected with each other.

4.2 Connecting Computers Wirelessly over WLAN

Using WLAN radio technology you can connect multiple computers with the FRITZ!Box wirelessly.

Please note the following before establishing a wireless connection between the computer and the FRITZ!Box:

- WLAN device

A computer to be connected to the FRITZ!Box via WLAN must be equipped with a WLAN device for it to support WLAN. A WLAN device can be an external WLAN adapter—like a USB stick, for example—or a device integrated in the computer. Many modern computers and notebooks come with a WLAN device integrated.

- WLAN security settings

In the FRITZ!Box, WLAN security settings are enabled upon delivery. Before a computer can establish a wireless connection to the FRITZ!Box, the WLAN security settings of the FRITZ!Box must be transferred to the WLAN device.

For this procedure the FRITZ!Box supports the two automatic methods AVM Stick & Surf and WPS (Wi-Fi Protected Setup). The security settings can also be transferred manually.



For more information on WLAN, see the section [The FRITZ!Box as a WLAN Base Station from page 44](#).

Establishing a WLAN Connection with AVM Stick & Surf

If you use a FRITZ!WLAN USB Stick from AVM as the WLAN device, you can use AVM Stick & Surf to establish a secure WLAN connection quickly and conveniently.

1. Switch on your computer.

2. Insert the your FRITZ!WLAN USB Stick into the USB port on the FRITZ!Box.

The WLAN security settings are transmitted to the FRITZ!WLAN USB Stick. The “Info” LED on the FRITZ!Box begins flashing quickly.

As soon as the “Info” LED stops flashing, transmission of the settings has been concluded.

3. Remove the FRITZ!WLAN USB Stick.
4. Now insert the FRITZ!WLAN USB Stick into the USB port of the computer.

The security settings will be adopted and the WLAN connection between the FRITZ!Box and the FRITZ!WLAN USB Stick will be established. As soon as the WLAN connection has been established the computer is connected to the FRITZ!Box.



See the AVM FRITZ!WLAN USB Stick manual for details.

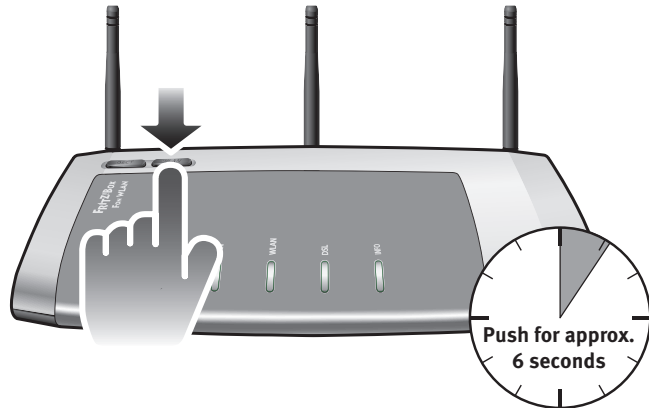
Establishing a WLAN Connection Using WPS

The FRITZ!Box supports WPS (Wi-Fi Protected Setup). WLAN devices that also support WPS can be connected with your FRITZ!Box securely using this method. All of the necessary WLAN security settings are transferred in the process. There are two kinds of WPS: the push-button method and the PIN method.

WPS with the Push-button Method

The push-button method (WPS PBC) can be used if your WLAN device is also equipped with a WPS button, or if WPS can be enabled via the control software of the WLAN device.

1. Press the “WLAN” button on the FRITZ!Box and hold it down for at least six seconds.



2. As soon as the “WLAN” LED begins flashing, enable the WPS function on the other WLAN device, either by pressing a button or in the device’s user interface (depending on the device). Activation must be started within two minutes.

The FRITZ!Box and the WLAN device now connect with each other automatically. The WLAN device adopts the security settings of the FRITZ!Box.

As soon as the WLAN connection has been established the computer is connected to the FRITZ!Box.

WPS with the PIN Method

If your WLAN device supports WPS, but does not have a button to start the push method nor any possibility to enable it in its control software, use the PIN method to establish the WLAN connection.

You can choose between two methods:

- the FRITZ!Box specifies the PIN
- the WLAN device specifies the PIN.

The FRITZ!Box Specifies the PIN

1. Open the FRITZ!Box user interface.
2. Select the “WLAN / Security” menu.
3. Go to the “WPS Quick Connection” page.
4. Enable the setting “WPS enabled”.
5. Select the option “PIN method (WPS-PIN), the FRITZ!Box specifies the PIN”.
6. The PIN will be displayed. Enter this PIN in the control software of the WLAN device.
7. Click “Start WPS”.

The “WLAN” LED on the FRITZ!Box flashes slowly, indicating that the WPS procedure has begun. Now a secure WLAN connection is being established between the FRITZ!Box and the WLAN device.

The WLAN Device Specifies the PIN

1. Open the FRITZ!Box user interface.
2. Select the “WLAN / Security” menu.
3. Go to the “WPS Quick Connection” page.
4. Enable the setting “WPS enabled”.
5. Select the option “PIN method (WPS-PIN), the WLAN device specifies the PIN”.
6. Now start the control software of the WLAN device. The program outputs a PIN for establishing a connection.
7. Enter this PIN in the FRITZ!Box user interface.
8. Click “Start WPS”.

The “WLAN” LED on the FRITZ!Box flashes slowly, indicating that the WPS procedure has begun. Now a secure WLAN connection is being established between the FRITZ!Box and the WLAN device.

Transferring the WLAN Security Settings Manually

The WLAN security settings for WLAN devices can also be transferred manually. Manual transfer is unavoidable if a WLAN device does not support any methods for transferring the security settings automatically.

For manual transfer the WLAN security settings have to be entered in the WLAN software.

WLAN devices are generally delivered with their own WLAN software, which is installed in the computer along with the WLAN device. By now many operating systems have WLAN software included. Integrated WLAN devices sometimes use the operating system's WLAN software.

Installing a WLAN Device

If you need to use a separate WLAN device because you do not have one integrated, then install the WLAN device in the computer along with the corresponding WLAN software. Please take note of the instructions in the documentation of the device.

Transferring WLAN Security Settings

The values for WLAN security preconfigured in the FRITZ!Box have to be transferred to the WLAN device.



If you would like to establish a WLAN connection using the values preset in the FRITZ!Box, then your WLAN device must support the WPA encryption procedure.

1. Start the WLAN software.

2. Enter the following values for the connection between the FRITZ!Box and the WLAN device:

SSID (name of the WLAN radio network)	FRITZ!Box 3270
Encryption method	WPA (TKIP) or WPA2 (AES-CCMP)
Encryption	WPA PSK or WPA2 PSK (AES)
WLAN key	The key is printed on the sticker attached to the bottom of the housing.
Network mode	Infrastructure

3. Confirm your entries using the relevant button in the user interface (for instance, “OK” or “Connect”).

Now your WLAN device and the FRITZ!Box are connected with each other wirelessly.

5 The FRITZ!Box User Interface

The FRITZ!Box has a user interface you can open in a web browser on your computer.

In the user interface you can set up the FRITZ!Box, enable or disable functions and receive information on the FRITZ!Box and on your connections.

5.1 Opening the User Interface

The FRITZ!Box user interface can be opened on every computer connected with the FRITZ!Box.

1. Start a web browser on your computer.
2. Enter fritz.box in the address line of the browser.

The FRITZ!Box user interface opens.



Entering the address fritz.box in the browser



If the user interface does **not** open, see the instructions on resolving errors in the section from [page 82](#).

The Wizard: Opening the User Interface for the First Time

When you open the user interface for the first time, a wizard starts to assist you in configuring the FRITZ!Box.

If you cancel the wizard, you can configure your FRITZ!Box without this wizard. You can change the settings configured with this wizard at any time.

For comprehensive information on configuring the many diverse functions of your FRITZ!Box, see the following chapters in this manual.

5.2 Protecting the User Interface with a Password

You can protect the user interface of the FRITZ!Box with a password. The password will be requested every time the user interface is opened. This protects the settings of your FRITZ!Box from unauthorized access.



We strongly recommend setting up and using password protection for the user interface.

Setting Up Password Protection

As long as no password protection has been set up, every time you open the user interface you will be prompted to enter a password. If you disabled this message, here is how to set password protection:

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Go to the “System / FRITZ!Box Password” menu.
3. Enter a password and save the password by clicking “Apply”.

Password protection is now enabled.



Be sure to remember the password! If you forget the password, the factory settings will have to be restored to your FRITZ!Box (see [page 94](#)). All of the settings you configured will be discarded.

Logging Off the User Interface

When password protection is enabled, you can log off the user interface at any time. To do so, click  **Log off**.

If you do not click on the user interface for a period of longer than ten minutes, you will be logged off automatically. The only pages excepted from this are those which are constantly updated, like the “Overview” page. No automatic logout will take place on these pages.

5.3 Saving the FRITZ!Box Settings

All of the settings you configure in your FRITZ!Box can be saved in a backup file on your computer. With this backup file you can restore your settings to the FRITZ!Box at any time or load your settings to another FRITZ!Box.

Saving and Restoring Settings

To save and restore your FRITZ!Box settings, use the “System / Save Settings” menu in the user interface. Here you can

- save your FRITZ!Box settings on the “Save” tab.
- restore all of your saved settings to **the same FRITZ!Box** on the “Restore” tab.
- load all of your saved settings to **another FRITZ!Box of the same model** on the “Restore” tab.
- load your saved settings to **another FRITZ!Box model** on the “Apply” tab. In this case you can select which settings are to be applied to the FRITZ!Box.



To load your saved settings to **another FRITZ!Box of the same model**, or to apply your FRITZ!Box settings to **another FRITZ!Box model**, the backup file must always be password-protected.

Instructions for saving, restoring and applying FRITZ!Box files are presented in the user interface’s Online Help.

6 Configuring an Internet Connection in the FRITZ!Box

Once you have connected the FRITZ!Box to your Internet connection, you must configure the Internet connection in the FRITZ!Box user interface so that the FRITZ!Box can establish the connection to your Internet Service Provider and connect to the Internet.

The sequence and number of steps required to configure your Internet connection depend on the kind of connection, the desired operating mode, and the Internet Service Provider.

6.1 Configuring an Internet Connection for DSL

If you have a DSL line, you received Internet account information from your DSL or Internet Service Provider. The Internet account information is required to configure the Internet connection.



Your Internet Service Provider also supplied information about the configuration of your Internet connection. Always perform the Internet connection setup as described by your provider.

Configuring an Internet Connection Automatically

If your Internet Service Provider arranges for the service of automatically configuring your Internet connection, the automatic configuration will be performed right after the FRITZ!Box is connected. No additional settings for the Internet connection have to be configured in the FRITZ!Box. To start automatic configuration, some providers require that you enter a start code.

Configuring the Internet Connection Using the Wizard

With the Wizard it is simple to configure the Internet connection.

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Select “Wizards” in the menu.
3. Click the “Check Internet Connection” Wizard and follow the instructions.

When the Wizard is finished, your Internet connection has been configured.

Configuring the Internet Connection Without the Wizard

You can also set up the Internet connection without the Wizard.

Choose this method if the FRITZ!Box is connected to a DSL modem or a DSL router, or integrated into an existing network.

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Enable the expert settings in the “System / Expert Mode” menu.
3. Select the “Internet / Account Information” menu and enter your account information.

Also take advantage of the Help available in the FRITZ!Box user interface.

6.2 Changing the Annex Setting of the FRITZ!Box

The FRITZ!Box cannot establish a connection to the DSL network. This is signaled by the continued flashing of the “Power” LED.

Cause

The kind of DSL (Annex A, B, M or J) set in the FRITZ!Box is not the same as the annex used on your DSL line.

Help

1. Contact your Internet Service Provider to find out which annex is used on your DSL line.
2. Connect a computer with the FRITZ!Box either wirelessly via WLAN or using a network cable.
3. Open the FRITZ!Box user interface.
4. Open the “Internet / DSL Information” and select the “Line Settings” page.
5. In the “Annex Settings” area, make sure that the annex working on your DSL line is set. Save your settings by clicking “Apply”.

After the annex setting has been changed, the FRITZ!Box restarts automatically. The connection to the DSL network has been established as soon as the “Power” LED stops flashing and remains lit up.

6.3 Configuring the Internet Connection for Cable

With an additional cable modem you can also use your FRITZ!Box 3270 on a cable connection. Then the Internet connection is established and controlled by the FRITZ!Box itself, so that in this operating mode, too, all FRITZ!Box functions (like Internet telephony, firewall) are available without restriction.

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Select “Wizards” in the menu.
3. Click the “Check Internet Connection” Wizard and follow the instructions.

6.4 Configuring the Internet Connection for the Mobile Telephone Network

With a USB modem you can also establish the Internet connection with your FRITZ!Box 3270 via the mobile telephone network. A USB modem for mobile Internet access (UMTS/HSPA) is required for this. The FRITZ!Box supports UMTS/HSPA modems from various manufacturers.

The USB modem is already installed on the USB port of the FRITZ!Box.

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. In the “Internet” menu, the sub-menu “Mobile Telephone Network” is displayed.



The “Mobile Telephone Network” menu is not available until the UMTS/HSPA modem has been connected to the FRITZ!Box. From this point on the menu is always available, even when the USB modem has been disconnected.

3. Configure the settings for your Internet connection over the mobile telephone network. For more information, see the Online Help of the FRITZ!Box.

When the mobile telephone network function is used, the FRITZ!Box user interface presents information about network availability, connection status and throughput.



Due to technical limitations on the part of the mobile telephone network providers, some limitations may arise for Internet telephone calls and for applications requiring an incoming connection. The same is true for using port forwarding, sharing USB storage memory, remote access via HTTPS, dynamic DNS and VPN. Contact your network provider for details on any restrictions that may apply.

6.5 Surfing the Net

Once you have set up the Internet connection in your FRITZ!Box, you can surf the Internet with any computer connected to the FRITZ!Box.

1. Start a web browser on your computer.
2. Enter in the address field the URL of the web page you would like to visit, for instance www.avm.de/en.

The requested Internet page is opened and displayed.

7 Firmware Update: Updating the FRITZ!Box Software

AVM provides free updates of the firmware for the FRITZ!Box. The firmware is the software stored in the FRITZ!Box that controls all of the FRITZ!Box functions.

Firmware updates contain further developments of existing FRITZ!Box functions and often also introduce new functions for your FRITZ!Box.

Finding New Firmware and Transferring It to the FRITZ!Box

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Click “Wizards” in the menu and start the “Update Firmware” Wizard.

The Wizard checks whether new firmware is available for your FRITZ!Box.

If the Wizard finds new firmware, it displays the version number of the firmware. Click the link under the firmware version to view information about further developments and new functions contained in the firmware update. Read this information before starting the firmware update.

3. To transfer new firmware to the FRITZ!Box, click “Start Firmware Update Now”.

The firmware update begins and the “Info” LED on the FRITZ!Box starts flashing.



Do not interrupt the power supply to the FRITZ!Box during the firmware update!

The firmware update is complete when the “Info” LED stops flashing.

8 The FRITZ!Box as an Internet Router

The FRITZ!Box connects computers in your home network with the Internet. This chapter explains the possibilities offered by using the FRITZ!Box as an Internet router and how to take advantage of them.

8.1 Child Protection: Restricting Internet Access

The child protection feature allows you to define access rules to the Internet for individual computers or Windows users. These access rules may include restrictions of Internet access time, filter lists and a list with blocked network applications.

- **Restrict Internet access time:** Using the time restriction you can restrict the amount of time the user can surf the web. You can define on which days of the week, at what times of day, and for how long a computer or Windows user is allowed to use the Internet connection.
- **Block or permit web sites:** you can use filter lists to define which Internet pages are allowed to be accessed and to which access is blocked. For instance, you can block all Internet pages the government has defined as offensive or harmful to minors.

You can create both filter lists, the whitelist and the blacklist. A whitelist contains all Internet pages to which access is allowed. A blacklist contains all Internet pages to which access is blocked.

- **Block network applications:** You can list network applications for which Internet access should be blocked. For instance, you can block Internet access for file-sharing software.

Child protection can be enabled for each computer individually, regardless of the computer's operating system.

You can also enable child protection individually in all Windows operating systems (Windows 7, Windows Vista and Windows XP). This option is very beneficial if a computer is used by multiple users.

Setting Up Child Protection in the FRITZ!Box

The child protection feature is available only if you have set up the Internet connection in the FRITZ!Box and established an Internet connection. Child protection is **not** available if you have configured the FRITZ!Box as a DSL modem or IP client.

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Select the “Internet / Filters” menu.
3. Set up the child protection feature, making use of the Online Help in the FRITZ!Box user interface.

8.2 Port Forwarding: Making Computers Accessible from the Internet

With default settings in the FRITZ!Box, programs on your computer and LAN cannot be accessed from the Internet. For a number of applications like online games and file sharing software, you have to make your computer accessible for other Internet users. In order to grant controlled access to your computer to other Internet users, you release certain ports for incoming connections. The ports serve to distinguish between running applications on a computer that has only one IP address.

Setting Up Port Forwarding in the FRITZ!Box

- Port Forwarding is set up in the “Internet / Permit Access” menu.
- Port Forwarding for IPv6 is also set up in the “Internet / Permit Access” menu, on the “IPv6” page. To see this page, make sure you enabled the expert mode in the “System / Expert Mode” menu.

Address for Accessing the FRITZ!Box

If you have enabled the ports for forwarding in the FRITZ!Box, other users can access your computer at the IP address assigned to your FRITZ!Box by the Internet Service Provider. This is a public IP address.

Here is how to determine the public IP address of the FRITZ!Box:

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Enable the expert settings in the “System / Expert Mode” menu.
3. Open any Internet page in order to establish an Internet connection.
4. The FRITZ!Box’s public IP address is displayed on the “Overview” page in the “Connections” area.



Every time the Internet connection is interrupted the Internet Service Provider re-assigns the IP address. The IP address may change in the process. Therefore it is a good idea to use dynamic DNS so that the IP address can always be reached under the same name. For more information, see the section [Dynamic DNS: Name Instead of IP Address on page 35](#).

8.3 Dynamic DNS: Name Instead of IP Address

Dynamic DNS is an Internet service that makes it possible for the FRITZ!Box to remain accessible from the Internet at all times under a fixed name, even though the public IP address changes.

You must register with a dynamic DNS provider to use this service. When you register, you agree on the fixed name (domain name) at which your FRITZ!Box should be accessible from the Internet. You also define a user name and password.

Every time the IP address changes, the FRITZ!Box transmits the new IP address to the dynamic DNS provider in the form of an update request. Then the domain name is assigned to the current IP address by the dynamic DNS provider.

Setting Up Dynamic DNS in the FRITZ!Box

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Make sure that the expert mode is enabled in the “System / Expert Mode” menu.
3. Select the “Internet / Permit Access” menu.
4. Select the “Dynamic DNS” page and set up dynamic DNS. Consult the Online Help available in the FRITZ!Box user interface for more information.

8.4 Remote Access over HTTPS

With this function it is possible to access the user interface of the FRITZ!Box from another location. With this feature you can configure settings in the FRITZ!Box or perform a firmware update using a computer that is not in your own network (LAN or WLAN).

Setting Up Remote Access over HTTPS in the FRITZ!Box

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Make sure that the expert mode is enabled in the “System / Expert Mode” menu.
3. Select the “Internet / Permit Access” menu.
4. Select the “Remote Access” page and set up dynamic DNS. For more information, see the Online Help.

8.5 Prioritization: Right of Way for Internet Access

Prioritization is a function you can use to specify that network applications and network devices be treated with higher or lower priority when they access the Internet connection. For example, you may wish to ensure that applications like IPTV and video on demand are always treated with higher priority than other applications. You can also specify that file-sharing applications like eMule and BitTorrent always have to wait behind online games.

Categories for Prioritization

There are three categories for prioritization: “Real-time applications”, “Prioritized applications” and “Background applications”. The categories are explained below.

Network applications and network devices are assigned to the categories using rules.

Real-time Applications

This category is suitable for applications with high demands on transmission speed and reaction times (for example, IPTV or video on demand).

- Network applications of this category always have priority over other applications accessing the Internet at the same time.
- When the Internet connection is working at full capacity, the network packets of the applications of this category will always be sent first. In this case data from network applications assigned to other categories, like “Prioritized applications”, will be transmitted later.
- If multiple network applications are assigned to this category, then they must share the available capacity.
- Whenever Internet telephony is included in this category, this application always has the highest priority, even over other real-time applications.

Prioritized Applications

This category is suitable for applications that require a fast reaction time (for example, company access, terminal applications, games).

- For network applications prioritized in this category, 90% of the FRITZ!Box’s upload bandwidth is available, as long as no application from the “Real-time applications” category requires bandwidth. The remaining 10% of the upload bandwidth is available for applications that are prioritized in lower categories or not prioritized at all.

- If multiple network applications are assigned to the “Prioritized applications” category, then they must share the available capacity.

Background Applications

This category is suitable for applications that do not require any high transmission speed and which are not time-critical (for example, peer-to-peer services or automatic updates).

- Network applications assigned to this category are always treated with the lowest priority when the Internet connection is working at full capacity. So whenever an application from a different category or a non-prioritized application requires the entire bandwidth, all background applications must wait until bandwidth capacity becomes available again.
- If no other network applications are active, then the background applications receive the entire bandwidth.

Prioritization Method in the FRITZ!Box

The following algorithm is used in the FRITZ!Box to send data packets according to their prioritization:

- Change in the order in which packets are sent to the Internet (upstream direction)

The order of the packets the FRITZ!Box receives from the Internet (downstream direction) cannot be changed.
- Discard low-priority packets in order to ensure the transmission of higher-priority packets. This algorithm is used whenever more packets are supposed to be sent to the Internet than the upstream transmission rate of the Internet connection allows.
- As long as no packets are being sent from higher-priority applications, the full transmission rate of the Internet connection is available for low-priority packets.

Setting Up Prioritization in the FRITZ!Box

In order to use prioritization, the expert mode must be enabled in the user interface of the FRITZ!Box.

1. Make sure that the expert mode is enabled in the “System / Expert Mode” menu.
2. Prioritization is set up in the “Internet / Filters / Prioritization” menu.

8.6 VPN: Remote Access to the Home Network

Via VPN ([see glossary](#)) a secure remote access to the network of the FRITZ!Box can be established. The VPN solution for the FRITZ!Box features the following:

- The VPN solution for the FRITZ!Box is based on the IPSec standard.
- Computer-LAN coupling and LAN-LAN coupling: VPN connections can be set up for individual remote computers or even for remote networks.
- A maximum of eight simultaneous active VPN connections is supported.
- The configuration files for the VPN connections are created using a separate program. The program is provided free of charge and can be downloaded from the AVM web site.
- A free VPN client for individual computers can also be downloaded from the AVM web site.

The AVM web site offers a Service Portal which presents comprehensive information on VPN in general and in connection with the FRITZ!Box. Visit this portal to obtain more detailed information.

www.avm.de/en/vpn

Setting Up VPN in the FRITZ!Box

1. Open the FRITZ!Box user interface.
2. Enable the expert settings in the “System / Expert Mode” menu.
3. Select the “Internet / Permit Access” menu.
4. Select the “VPN” page.

See the Online Help of the FRITZ!Box to set up VPN.

Supplementary Software for VPN

All of the information required for a VPN is saved in a configuration file. The terminals involved in any VPN must receive this file.

If an individual computer is integrated into a network via a VPN, the computer must have a VPN client installed.

- “Configure FRITZ!Box VPN Connection” Wizard

AVM provides the “Configure FRITZ!Box VPN” software for creating configuration files. This program is a Wizard that takes you step by step through the VPN configuration. All of the necessary VPN settings, like the encryption method and access rules, are set automatically. The resulting configuration files must be imported to the respective terminals of the VPN tunnel. At the terminal with the FRITZ!Box the configuration file is then imported to the FRITZ!Box. The VPN parameters in these files can be adjusted manually to connect to products by other manufacturers.
- The “FRITZ!VPN” VPN Client

AVM offers the “FRITZ!VPN” software as a VPN client.

Both the Wizard and the client can be downloaded free of charge from the VPN Service Portal on the AVM web site:

www.avm.de/en/vpn

8.7 DNSSEC: Security for DNS Queries

DNSSEC is short for Domain Name System Security Extensions. As the name says, this is an extension of DNS, the domain name system.

DNSSEC ensures that both the DNS server and the information returned by the DNS server are authentic, or genuine.

Support with the FRITZ!Box

The FRITZ!Box supports DNSSEC queries over UDP.

The FRITZ!Box has a DNS proxy. The computers in the home network use the FRITZ!Box as a DNS server. The FRITZ!Box forwards DNSSEC queries from the home network to the Internet. The FRITZ!Box forwards DNSSEC responses from the Internet to the home network. The DNSSEC information must be validated on the computer in the home network. For this DNSSEC must be supported in the operating system.

Security with DNSSEC

When a home user surfs the web, she or he sends queries to the Internet by entering URLs in the address line of his browser. A URL is the name of a web site that is easy to remember, such as avm.de/en. Every query is sent to the DNS server first. The DNS server resolves the URL into the corresponding IP address. There is one unambiguous IP address for every URL.

The home user relies on the authenticity of the IP address returned by the DNS server. Authentic means that the response is the IP address of the desired web site, and not a faked IP address that leads to a fake web site. DNSSEC can ensure that the returned addresses are authentic.

8.8 IPv6: The New Internet Protocol

IPv6 stands for Internet protocol version 6 and is the successor to IPv4.

The FRITZ!Box supports the new IPv6 web protocol and can already establish IPv6 connections today:

- IPv6 support can be switched on in the FRITZ!Box user interface, in the “Internet / Account Information” menu.
- For simultaneous use of IPv6 and IPv4, the FRITZ!Box supports dual-stack and dual-stack lite. This means that the FRITZ!Box can communicate with both IPv4 and IPv6 domains in the Internet.
- The FRITZ!Box supports native IPv6 and IPv6 with a tunnel protocol. Native IPv6 means that your Internet Service Provider supports IPv6 directly on your line.

IPv6-capable Services in the Home Network

- FRITZ!NAS access via SMB or FTP/FTPS
- access to the user interface with http or https over IPv6
- The DNS resolver of the FRITZ!Box supports queries for IPv6 addresses (AAAA records) and can query the upstream DNS resolver of the Internet Service Provider over IPv6.
- The globally valid prefix is distributed via router advertisement.
- For guest access to the WLAN, the home network and WLAN guests are separated by IPv6 subnetworks.
- UPnP, UPnP AV media server

IPv6-capable Services in the Internet

- FRITZ!NAS access via FTPS
- completely closed firewall to protect against unwanted data from the Internet (Stateful Inspection Firewall)
- automatic provisioning (TR-069)
- time synchronization over NTP (Network Time Protocol)
- remote access via https

Setting Up IPv6 in the FRITZ!Box

1. Open the FRITZ!Box user interface.
2. Enable the expert settings in the “System / Expert Mode” menu.
3. Then select the “Internet / Account Information” menu.
4. Select the “IPv6” page and set up IPv6 in the FRITZ!Box. Consult the Online Help of the FRITZ!Box user interface for more information.

Setting Up IPv6 on the Computer

You can establish connections in the IPv6 range of the Internet only if IPv6 is installed and enabled on the computers in your home network.

- IPv6 is already installed and enabled in the Windows 7 and Windows Vista operating systems.
- IPv6 is not installed and enabled in standard Windows XP. You must install and enable IPv6 in order to use it. The IPv6 installation requires Service Pack 2 for Windows XP.
- IPv6 has been available in the Mac OS X operating systems since Mac OS 10.

9 The FRITZ!Box as a WLAN Base Station

The FRITZ!Box supports WLAN (Wireless Local Area Network) technology. In this chapter you will learn how you can use WLAN with the FRITZ!Box.

9.1 Security

Security is of utmost importance within radio networks.



Radio signals can also be received outside of office or residential spaces and abused for criminal purposes.

Therefore it is important that no unauthorized users can register in a WLAN to use its Internet access or shared network resources.

FRITZ!Box includes settings on various levels that contribute to the security of your WLAN and thus to the security of your computers.

Wireless Network Name (SSID)

In the factory settings of the FRITZ!Box, the name of the wireless network (SSID) is set to “FRITZ!Box 3270”.



It may occur that an additional device with the same FRITZ!Box network name is located in the vicinity of your FRITZ!Box. Therefore we recommend changing the preset radio network name.

9.2 Guest Access: WLAN Connection for Guests

You can connect computers with the FRITZ!Box via WLAN so that they can access the Internet without being integrated in the home network of the FRITZ!Box. This function is called “guest access”.

Your guests can use the guest access, for instance, to surf the web with a notebook and to receive e-mail.

Prerequisites for Guest Access

The FRITZ!Box must be connected directly to the DSL line.

Guest Access Properties

- The guest radio network is a separate radio network with its own name (SSID). It is independent of the wireless network of the FRITZ!Box that integrates computers in the home network.
- Computers connected via guest access are not part of the home network.
- The guest network is secured with its own network key. This network key can be changed as desired without affecting the computers in your home network.

Setting Up Guest Access in the FRITZ!Box

1. Open the FRITZ!Box user interface.
2. Make sure that the expert mode is enabled in the “System / Expert Mode” menu.
3. Make sure that the wireless radio network (WLAN) is enabled in the “WLAN / Radio Network” menu.
4. Select the menu “WLAN / Guest Access” and configure the guest radio network. For more information, see the Online Help of the FRITZ!Box.

9.3 Setting Up Night Service for WLAN

In the FRITZ!Box you can set up night service for the WLAN radio network. Then the FRITZ!Box switches to hibernation at specified times and turns off the radio network. This has the following advantages:

- reduced power consumption when idle
- time-controlled Internet access: with night service you can ensure that your children are only allowed to surf the web until a certain time of day

Switching Night Service for WLAN On and Off

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Select the “System / Night Service” menu.
3. Enable the “Use schedule for WLAN radio network” option.
4. Enable or disable the option “The radio network cannot be switched off until no more WLAN devices are active”.

Option enabled: The radio network remains switched on until all wireless connections between the FRITZ!Box and other WLAN devices have been ended.

Option is disabled: The radio network is switched off immediately at the start of the specified period.
5. Define the days and times at which the FRITZ!Box WLAN radio network should be switched off.
6. Save your settings by clicking “Apply”.

Night service for WLAN is now enabled. To disable night service, remove the checkmark in front of “Use schedule for WLAN radio network” and click “Apply”.

Switching On WLAN during Night Service

The WLAN radio network of the FRITZ!Box can be switched back on at any time during night service:

Press the “WLAN” button on the FRITZ!Box. The WLAN radio network will be switched on.

9.4 Increasing the Range of the WLAN Connection

The range of a WLAN radio network is influenced by various external circumstances. The following factors have an especially strong influence on the distance over which your FRITZ!Box can establish a stable, high-throughput wireless connection:

- the WLAN device used
- structural conditions
- the number of devices operating near the access point in the same frequency range.

If needed, you can extend the range of your WLAN radio network with a WLAN repeater, for instance with the FRITZ!WLAN Repeater N/G or FRITZ!WLAN Repeater 300E from AVM. A WLAN repeater is a supplementary device that is not included in the FRITZ!Box package.

Instead of using a WLAN repeater, you can set up a Wireless Distribution System. For this you need, in addition to the FRITZ!Box, another WLAN access point that is configured as a WDS repeater (see [page 48](#)).

Using the FRITZ!WLAN Repeater

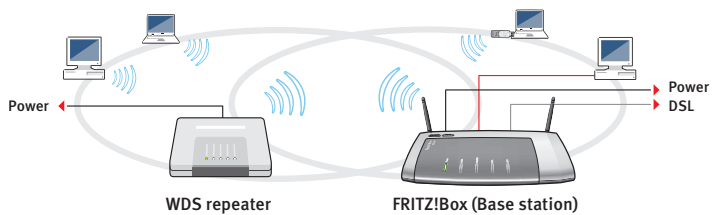
With the FRITZ!WLAN Repeater N/G from AVM you can extend the range of your WLAN radio network quickly and easily, for instance to overcome structural conditions that are characterized by thick materials and heavy shielding. The FRITZ!WLAN Repeater N/G supports all common WLAN standards, is especially easy to install and can be operated at any 230-V power outlet. For more information on the FRITZ!WLAN Repeater N/G, see the web site at:

www.avm.de/en/Produkte/FRITZ_WLAN/FRITZ_WLAN_Repeater_N_G

Setting Up a WDS

To use WDS (Wireless Distribution System) to increase the range of your WLAN radio network, you need another WLAN base station in addition to the FRITZ!Box. This can be a second FRITZ!Box or any other WLAN base station that supports WDS. The first WLAN base station then works as a WDS base station and the second as a WDS repeater.

The WDS base station and WDS repeater are connected to each other via WLAN. The WDS base station then can use the WDS repeater to reach even computers that are outside its own range, but within the range of the WDS repeater.



WDS: Expanding the WLAN range using a WDS repeater

Note the following for WDS configuration:

- To expand the range of your wireless network, you need at least one additional WLAN base station. The wireless network of your FRITZ!Box can be expanded to a WDS (Wireless Distribution System) with up to three WLAN base stations.
- All WLAN base stations implemented in the WDS must support WDS and be configured for this technology.
- All WLAN base stations implemented as repeaters in the WDS must be located within the radio range of the WDS base station.
- The FRITZ!Box can function as a WDS base station to establish the Internet connection for other WDS repeaters, or as a WDS repeater to expand the range of a WDS base station.

- All WDS connections between the WDS base station and the WDS repeaters must be secured using the same encryption (e.g. WPA/WPA2). **Note that the WPA2 encryption method is available only when your network consists of AVM devices, since in the WLAN standard only WEP encryption has been specified for WDS connections.**
- All WLAN base stations in the WDS must use the same radio channel.
- Every WLAN base station participating in the WDS fulfills the tasks of a WLAN access point for its WLAN clients. This means that the WLAN clients see each WLAN base station with an individual name (SSID) and individual encryption settings.

If you use the WLAN control software provided in Windows 7, Windows Vista or by the Windows XP Service Pack 2 on your WLAN clients, you can assign the same SSID and the same encryption settings to different WLAN base stations. Each client can then automatically register at the WLAN base station with the best availability.

- Each IP address may be assigned only once in the wireless network.

9.5 WLAN Standards

The WLAN standards IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n and IEEE 802.11i were developed by the Institute of Electrical and Electronic Engineers (IEEE).

The IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n standards define the throughput within a wireless radio network. IEEE 802.11i is a security standard.

Standards for the Throughput Rate

Data Throughput

The throughputs listed differentiate between gross and net transmission rates. The net speed describes the transmission rate of the user data.

The FRITZ!Box supports your choice of the standards IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n. WLAN devices based on one or more of the standards listed can be used for WLAN connections with the FRITZ!Box.

Standard	Frequency Band	Gross Data Throughput up to	Net Data Throughput up to
802.11b	2.4 GHz	11 Mbit/s	5 Mbit/s
802.11g	2.4 GHz	54 Mbit/s	25 Mbit/s
802.11a	5 GHz	54 Mbit/s	25 Mbit/s
802.11n	2.4 / 5 GHz	300 Mbit/s	150 Mbit/s

The standards are intended for different frequency bands.

IEEE 802.11a

Because this standard works exclusively in the seldom used 5-GHz range, it offers the opportunity to transmit data relatively free of interference from external influences. WLAN devices that support 802.11a are much less common than devices that work in accordance with the 802.11b/g standard.

IEEE 802.11b

With a maximum throughput rate of 11 Mbit/s, this is the oldest WLAN standard. Older WLAN devices of the first generation can communicate with the FRITZ!Box using 802.11b. However, if the WLAN device supports newer standards such as 802.11g, the latest standard should be used.

IEEE 802.11g

This is currently the most common WLAN standard. It communicates with a maximum of 54 Mbit/s gross in the 2.4-GHz frequency range (ISM) and guarantees broad compatibility with many WLAN devices.

However, due to heavy use of the 2.4-GHz range, interference is more common than in the less-used 5-GHz range.

IEEE 802.11n

This standard allows for high throughput rates and ranges. The FRITZ!Box supports 802.11n in the 2.4-GHz frequency band, or, if desired, also in the 5-GHz frequency band. Modulation processes and antenna techniques like MIMO (Multiple Input, Multiple Output) use whichever frequency band is available more effectively than the older standards.



The use of the 802.11n standard—and thus the availability of higher throughput rates—is possible only if the WLAN connection is secured using the WPA2 security mechanism (AES-CCMP).

Thanks to compatibility with the 802.11g standard, you can also continue to use older WLAN devices.

Setting the Right Standard in the FRITZ!Box

The throughput rate that can be achieved in your WLAN radio network depends on the WLAN standards used by the integrated WLAN devices. These WLAN standards must also be set in the FRITZ!Box. Proceed as follows to check which WLAN standards are set and change them if needed:

1. Open the FRITZ!Box user interface.
2. Make sure that the expert mode is enabled in the “System / Expert Mode” menu.
3. Open the “WLAN / Radio Channel” menu and select “Adjust radio channel settings” to make the desired changes.



Note the following for the configuration of this setting:

- In order to communicate with each other, the FRITZ!Box and all WLAN devices must work in the same frequency band.
- The standard you configure in the FRITZ!Box must be compatible with the standards of all WLAN devices used in the WLAN.

Make a note of which standards the WLAN devices in your network are compatible with and then adjust the FRITZ!Box settings according to the following information:

- Your radio network integrates only WLAN devices that are compatible with one or both of the following standards:

802.11n

802.11g

Set the following mode in the FRITZ!Box:

Mode: 802.11n+g

The 2.4-GHz frequency band will be used.

- Your radio network integrates only WLAN devices that are compatible with one or both of the following standards:

802.11b

802.11g

Set the following mode in the FRITZ!Box:

Mode: 802.11b+g

The 2.4-GHz frequency band will be used.

- Your radio network integrates only WLAN devices that are compatible with one or several of the following standards:

802.11n

802.11g

802.11b

Set the following mode in the FRITZ!Box:

Mode: 802.11n+g+b

The 2.4-GHz frequency band will be used.

- Your radio network integrates only WLAN devices that are compatible with one or both of the following standards:

802.11n

802.11a

Set the following mode in the FRITZ!Box:

Mode: 802.11n+a

The 5-GHz frequency band will be used.

The Standard for Security

IEEE 802.11i

The WPA2 security mechanism is defined in the IEEE 802.11i standard. WPA2 is an extension of the familiar security mechanism WPA (Wi-Fi Protected Access).

The main feature of the extension of WPA to WPA2 is the AES-CCMP encryption process.

Mechanism	Encryption
WPA	TKIP (Temporary Key Integrity Protocol)
WPA2	TKIP AES-CCMP based on the extremely secure AES (Advanced Encryption Standard) procedure. CCMP (Counter Mode with CBC-MAC Protocol) defines how the AES procedure is applied to WLAN packets.

FRITZ!Box supports the AES encryption procedure as part of the WPA2 mechanism, and the TKIP encryption procedure as part of the WPA mechanism. This means that the FRITZ!Box can be used in combination with any WLAN devices that also support WPA2 with AES or WPA with TKIP.

9.6 Frequency Ranges

WLAN uses the frequency ranges at 2.4 GHz and 5 GHz as its transmission range.

With the FRITZ!Box you can establish WLAN connections in either the 2.4-GHz or the 5-GHz frequency range.

2.4-GHz Frequency Band

In the 2.4-GHz frequency band WLAN works in the same range as Bluetooth, microwave devices and various other devices like radio-controlled toys, garage-door openers and video bridges. This means that interference may occur within WLANs operated in the vicinity of such devices. Generally this has adverse effects on the transmission rate, including aborted connections.

In the 2.4-GHz frequency range the European regulation authorities have designated 13 channels for WLAN. A channel can have a bandwidth of 20 MHz (throughput up to 130 Mbit/s) or 40 MHz (throughput of up to 300 Mbit/s).

Channels located directly next to each other in the 2.4-GHz band may overlap and result in mutual interference. For instance, if several WLANs are operated close to each other in the 2.4-GHz frequency range with a bandwidth of 20 MHz, a distance of at least five channels should be left empty between each two channels used. This means that if channel 1 is selected for one WLAN, the channels 6 through 13 can be selected for a second WLAN. This maintains the minimum distance between channels.

Should interference in a WLAN persist, the first step should be to select a different channel.

WLAN Autochannel

With the WLAN autochannel function, the FRITZ!Box automatically searches for the channel subject to the least interference. This process takes into consideration interference from radio networks in the vicinity (WLAN base stations) and potential sources of interference (for instance video bridges,

baby monitors, microwave ovens). Should problems with interference persist despite this function, try to identify the source of interference and switch it off manually.

Additional tips on interference in the WLAN radio network are presented in the section [Ruling Out Interference Caused by Other Wireless Networks from page 92](#).

5-GHz Frequency Band

The FRITZ!Box can operate in the 5-GHz frequency band as an alternative. This frequency range is used much less often than the most common 2.4-GHz frequency range.

In the 5-GHz frequency band the FRITZ!Box supports automatic channel switching by DFS (Dynamic Frequency Selection). DFS ensures that the channels from 52 to 140 are kept free for higher-priority users, like weather radar systems. If you are operating your FRITZ!Box in one of these channels, it monitors the selected channel periodically for higher-priority users, and, if necessary, switches to a different channel. Note that the FRITZ!Box waits up to ten minutes, as legally required, before occupying a free channel. During this period you cannot register any WLAN devices. The WLAN connection is then established automatically. For more information, see the section [Avoiding WLAN Channels with DFS on page 91](#).

A prerequisite for use of the 5-GHz frequency band is that all WLAN devices in the network support this frequency range in accordance with the IEEE 802.11a or IEEE 802.11n standard.

2.4 GHz or 5 GHz

The FRITZ!Box works in the wireless network either in the 2.4-GHz range or in the 5-GHz range, but not parallel in both frequency ranges at the same time.

Bandwidth

In both frequency ranges you can select between channel bandwidths of 20 MHz or 40 MHz (exception: channel 140 in the 5-GHz frequency band). The FRITZ!Box initially attempts to select a channel with 40 MHz bandwidth (throughput up to 300 Mbit/s). If this is not possible due to interference or

channels already being used by other WLANs in the vicinity, the FRITZ!Box automatically switches temporarily to a channel with 20 MHz bandwidth. Greater bandwidth provides for higher data throughput:

Bandwidth (MHz)	Maximum Data Throughput (Mbit/s)
20	130
40	300

Increasing bandwidths also increases the probability of interference by wireless networks in the vicinity. Large bandwidths reduce the frequency range available to other wireless networks in the vicinity.

Allocation of the WLAN Channels in the 2.4-GHz Range

Channel	Frequency (GHz)	Channel	Frequency (GHz)
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467
6	2.437	13	2.472
7	2.442		

Allocation of the WLAN Channels in the 5-GHz Range

Channel	Frequency (GHz)	Channel	Frequency (GHz)
36	5.18	108	5.54
40	5.20	112	5.56
44	5.22	116	5.58
48	5.24	120	5.60
52	5.26	124	5.62
56	5.28	128	5.64
60	5.30	132	5.66
64	5.32	136	5.68
100	5.50	140	5.70 (20 MHz band-width only)
104	5.52		

10 The FRITZ!Box Home Network

The FRITZ!Box connects your network devices, USB devices and storage devices in what we call a FRITZ!Box home network. In the home network the FRITZ!Box makes data like images, music and videos available to all connected users and allows them to share a printer.

Network Devices

Network devices include, for instance, computers, game consoles and smartphones that are connected with the FRITZ!Box via a network cable connection or via WLAN.

All network devices can access each other's folders released for sharing, and share connected USB devices and available memory.

If you would like to learn more about the possibilities of network devices in your FRITZ!Box home network, continue reading in the chapter [Network Devices in the FRITZ!Box Home Network from page 60](#).

USB Devices

USB devices include, for instance, printers, multi-function devices, and flash memory on the USB ports of the FRITZ!Box.

Connected USB devices can be used jointly and simultaneously by all network devices of your FRITZ!Box home network.

For more information about how to best configure USB devices in your home network and how to use them securely, see the chapter [USB Devices in the FRITZ!Box Home Network from page 71](#).

Storage (NAS)

The memory of the FRITZ!Box includes storage media like flash memory or hard drives connected to the USB ports of the FRITZ!Box.

What is more, the FRITZ!Box can manage online storage configured on the server of your telecommunications provider.

For more information about how to access the memory in your FRITZ!Box home network safely and conveniently, see the chapter [Accessing USB Memory from page 72](#).

11 Network Devices in the FRITZ!Box Home Network

All network devices connected with the FRITZ!Box comprise a network. Network devices include, for instance, computers, game consoles and smartphones. The devices can be connected with the FRITZ!Box by cable or wirelessly. This chapter describes the network settings in the FRITZ!Box and how you can change them. You will also learn how you can change the IP settings for the computer in the most common operating systems.

11.1 Network Settings in the FRITZ!Box

The FRITZ!Box is delivered with preconfigured network settings. According to these settings, all network devices connected with the FRITZ!Box are located in a single network.

The network settings can be changed and adapted to your conditions and needs. But you should do so only if you are well versed in networking technology.



The Glossary (from [page 112](#)) explains concepts and terminology having to do with IP networks.

Network Overview

The FRITZ!Box user interface shows an overview with all of the devices and users connected with the FRITZ!Box.

The network overview “Devices and Users” is found in the menu “Home Network / Network”.

For each user and each network device, you find an entry in the network overview. The columns have the following meanings:

Icon	Each name is preceded by a green LED if the device is actively connected with the FRITZ!Box, but currently not using the Internet connection. Any device using the Internet connection appears with a green-blue globe icon in front of its name.
Name	This column displays the name under which the user or the network device is known to the FRITZ!Box. The names of network devices can be changed by clicking the button to edit the entry.
IP Address	For network devices, also displayed is the IP address with which the device is integrated into the FRITZ!Box network.
Connection	The WLAN icon is displayed for wireless connections.
Properties	This column indicates whether port forwarding or child protection is enabled for the respective user or network device.
	Button for editing the entry The button opens the entry in editing mode. This view displays information about the network device, for instance on child protection or port forwarding settings. The name of the device in the FRITZ!Box can be changed here.
	Button for deleting the entry Users or network devices that do not have an active connection to the FRITZ!Box can be deleted from the network overview by clicking this button.

Always Assigning the Same IP Address

The editing mode for network devices includes the setting “Always assign this network device the same IP address”.

When this setting is enabled for a network device, the DHCP server of the FRITZ!Box will always assign the same IP address to this device each time the connection is established.

Starting the Computer – Wake on LAN

The editing mode for network devices that are connected with the FRITZ!Box via a network (LAN) port includes the “Start Computer” button. Use this button to start computers that support wake on LAN.

With the wake on LAN function you can start computers in your FRITZ!Box via the Internet. For instance, you can access a computer at any time using remote maintenance software, without wasting electricity by keeping the computer switched on permanently.

IP Settings in the FRITZ!Box

The IP settings of the FRITZ!Box are preset upon delivery with the following values:

FRITZ!Box Factory Settings	
IP address	192.168.178.1
Subnet mask	255.255.255.0
DHCP server	enabled

The IP address and the corresponding subnet mask yield the following values:

Network address of the subnet	192.168.178.0
Entire IP address range for the computers	192.168.178.2 - 192.168.178.254

The following addresses cannot be assigned because they are reserved for certain purposes:

This IP address is used by the FRITZ!Box itself	192.168.178.1
This IP address is the broadcast address used to send messages into the network	192.168.178.255

IP Address in the FRITZ!Box

Upon delivery the FRITZ!Box is assigned the following IP address:

192.168.178.1

If you would like to change the IP address, please read through the following sections.

When Does It Make Sense to Change the IP Address?

You should change the IP address of the FRITZ!Box if the following apply to your network:

- You have an existing local IP network, one subnet with several computers.
- Fixed IP addresses are registered in the network settings of the computer, and you do not want to or are not permitted to change these addresses.
- You want to connect the FRITZ!Box to the local IP network in order to make the FRITZ!Box features available to all of the computers in the IP network.

Reserved IP Addresses

The entire IP network 192.168.180.0 in the FRITZ!Box is reserved for internal purposes.

IP addresses from this network may **not** be assigned to the FRITZ!Box.

DHCP Server of the FRITZ!Box

The FRITZ!Box is equipped with its own DHCP server. The DHCP server is enabled by default in the factory settings. The following range of IP addresses is reserved for the DHCP server in the factory settings:

192.168.178.20 - 192.168.178.200

This IP address can be changed as needed.

Every time the operating system on a computer connected with FRITZ!Box is started, the DHCP server assigns it an IP address from the IP address range of the DHCP server.



Only one DHCP server may be active within any network.

Assigning the IP addresses via the DHCP server ensures that all of the computers connected with the FRITZ!Box are located in the same IP network.



The computers can receive their IP addresses from the DHCP server only if the setting “Obtain an IP address automatically” is enabled in the their IP settings. For more information, see the section [Obtaining an IP Address Automatically from page 66](#).

Fixed IP Addresses when the DHCP Server Is Enabled

If you would like to configure fixed IP addresses on individual computers connected with the FRITZ!Box despite the enabled DHCP server, please note the following:

- The IP addresses must be from the IP network of the FRITZ!Box.
- The IP addresses may not come from the address range of the DHCP server.
- Each IP address can be assigned only once.

Disabling the DHCP Server

You can disable the DHCP server.

To make sure that all computers remain in the same IP network when the DHCP server is disabled, you must enter the IP addresses manually in the computers’ network settings. First disable the option “Obtain an IP address automatically” and then enter the IP address manually in the appropriate field.

In the case of the preset IP address of the FRITZ!Box, the following IP addresses are available for assignment to the computers:

192.168.178.2 - 192.168.178.254



Here too: each IP address can be assigned only once.

Changing Network Settings

In order to change the network settings of the FRITZ!Box, the Expert Mode must be enabled in the user interface:

1. Select the “System / Expert Mode” menu and enable “Show expert settings”.
2. Select the “Home Network / Network” menu.
3. Select the “Network Settings” page.
4. Click the “IP Addresses” button.
The “IP Settings” page is opened.
5. Make the desired changes and then confirm with “OK” so that all changes will be applied.



Please note that changes to the network settings in the FRITZ!Box may make it necessary to adjust the network settings of your computers so that you can continue to access the FRITZ!Box user interface.

UPnP Settings

The Universal Plug-and-Play (UPnP) service included in your FRITZ!Box provides status information about the FRITZ!Box to all connected computers. Programs with UPnP support on these computers can receive this information and use them to display the status of the FRITZ!Box (e.g., connection status, data transmission). UPnP service thus allows you to monitor your FRITZ!Box from a connected computer.

Here is how to change the UPnP settings:

1. Open the FRITZ!Box user interface (see [page 25](#)).
2. Make sure that the expert mode is enabled in the “System / Expert Mode” menu.
3. Configure the UPnP settings in the “Home Network / Network” menu on the “Programs” page.

11.2 Obtaining an IP Address Automatically

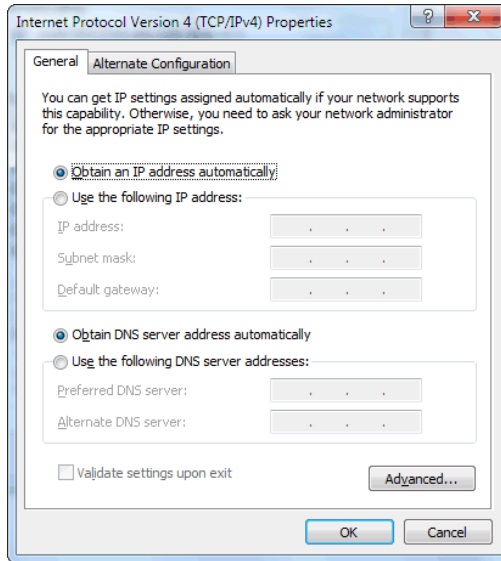
The FRITZ!Box has its own DHCP server, which assigns IP addresses to the connected computers. The connected computers must be configured such that they can receive their IP addresses automatically. The steps for checking and adjusting this option differ among the operating systems. See the relevant section for your operating system.



If FRITZ!Box is operated in a network, no other DHCP server may be activated in this network.

Obtaining an IP Address Automatically in Windows 7

1. Click the “Start” button in the task bar and select the “Control Panel / Network and Internet”.
2. Under “Network and Sharing Center”, click “View network status and tasks”.
3. From the left column, select the “Change adapter settings” command.
4. Select the LAN connection between your computer and the FRITZ!Box. Click the right mouse button and select “Properties”.
5. Under “This connection uses the following items”, select the “Internet Protocol Version 4 (TCP/IPv4)” entry and click “Properties”.
6. On the “General” tab, enable the options “Obtain an IP address automatically” and “Obtain DNS server address automatically”.



Properties of the Internet protocol (TCP/IP)

7. Confirm your selection by clicking “OK”.

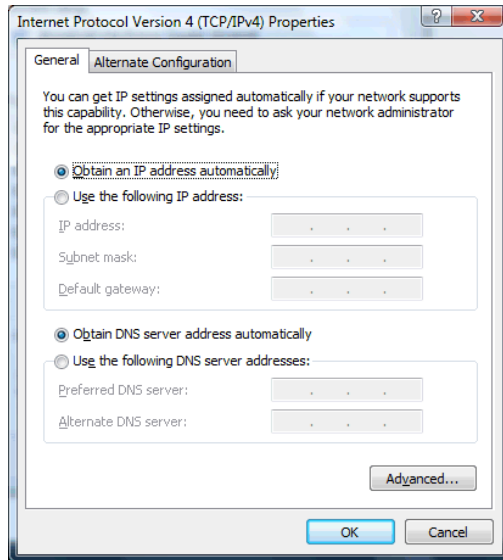
Repeat steps 5 through 7 for the “Internet Protocol Version 6 (TCP/IPv6)” as well.

The computer now receives an IP address from the FRITZ!Box.

Obtaining an IP Address Automatically in Windows Vista

1. Click the “Start” button in the task bar and select the “Control Panel / Network and Sharing Center”.
2. From the “Tasks”, select “Manage network connections”.
3. In the “LAN or High-Speed Internet” area, select the LAN connection between your computer and the FRITZ!Box. Click the right mouse button and select “Properties”.
4. If the “User Account Control” window is displayed, click “Continue” in this window.
5. Under “This connection uses the following items”, select the “Internet Protocol Version 4 (TCP/IPv4)” entry and click “Properties”.

6. On the “General” tab, enable the options “Obtain an IP address automatically” and “Obtain DNS server address automatically”.



Properties of the Internet protocol (TCP/IP)

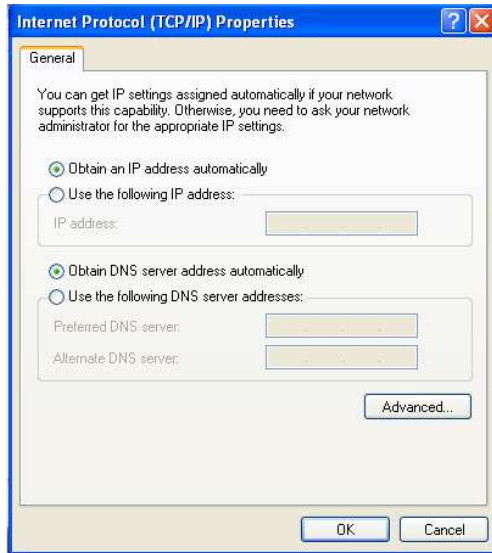
7. Confirm your selection by clicking “OK”.

If necessary, repeat steps 5 through 7 for the “Internet Protocol Version 6 (TCP/IPv6)” as well.

The computer now receives an IP address from the FRITZ!Box.

Obtaining an IP Address Automatically in Windows XP

1. Go to “start / Control Panel / Network and Internet Connections / Network Connections” and double-click the LAN connection icon of the network adapter connected to the FRITZ!Box.
2. Click the “Properties” button.
3. Select “Internet Protocol (TCP/IP)” in the list of items used in this network connection and click “Properties”.
4. On the “General” tab, enable the options “Obtain an IP address automatically” and “Obtain DNS server address automatically”.



Properties of the Internet protocol (TCP/IP)

5. Confirm your selection by clicking “OK”.

The computer now receives an IP address from the FRITZ!Box.

Obtaining an IP Address Automatically in Mac OS X

1. Select the “System Preferences” in the Apple menu.
2. In the “System Preferences” window, click the “Net-
work” icon.
3. In the “Network” window, select the “Built-in Ethernet”
entry from the “Show:” drop-down list.
4. Switch to the “TCP/IP” settings page and select the “Us-
ing DHCP:” option from the “Configure IPv4” drop-down
menu.
5. Click “Apply Now”.

The computer now receives an IP address from the FRITZ!Box.

Obtaining an IP Address Automatically in Linux

For comprehensive information and tips on the topic of network settings in Linux, see, for example:

<http://www.tldp.org/HOWTO/NET3-4-HOWTO-5.html>

12 USB Devices in the FRITZ!Box Home Network

The FRITZ!Box has a USB port to which you can connect various USB devices. All network devices in the FRITZ!Box home network can use these USB devices jointly and simultaneously.

This chapter describes how to share a printer in the network, which USB devices can be used in your FRITZ!Box home network, and how to use these devices safely.

12.1 Power Supply for USB Devices

You can connect USB devices with the following properties to the FRITZ!Box:

- Some USB devices require more than one USB port for operation, for instance, hard drives with a USB Y cable. Connect this type of USB devices to the FRITZ!Box using a USB hub with its own power supply.
- The total current consumption of connected USB devices without their own power supply may not exceed 500 mA. Check the rating plates of the connected USB devices.

USB devices that exceed the total current consumption of 500 mA can be connected to the FRITZ!Box using a USB hub with its own power supply.

12.2 USB Devices on the FRITZ!Box

These USB devices can be connected to the FRITZ!Box:

- You can connect up to four USB storage media like hard disks, USB flash drives or card readers.
- USB storage media must use the file systems EXT2, FAT, FAT32 or NTFS. On storage media with the FAT and FAT32 file systems you can use files up to a size of 4 GB. In the NTFS file system there is no limit to the size of files that can be used.
- You can connect **one** standard USB printer or **one** all-in-one device with scanner and fax function. The complete range of functions available in a all-in-one printers

device is guaranteed only with the USB remote connection of the FRITZ!Box (see also: [Sharing a USB Printer on page 73](#)).

- You can connect a USB stick from the FRITZ!WLAN USB Stick series by AVM to conveniently establish secure WLAN connections using AVM Stick & Surf (see: [Establishing a WLAN Connection with AVM Stick & Surf on page 19](#)).

12.3 Using USB Devices Safely

Follow the instructions below about how to use USB devices on your FRITZ!Box.

- The FRITZ!Box can not defend the USB memory from external influences. This means that voltage spikes or drops, like those that occur during electrical storms, may lead to data losses on connected USB memory media. We recommend making regular backups of the USB memory contents to avoid any losses.
- Whenever you want to remove USB devices from the FRITZ!Box, go to the “Home Network / USB Devices” area in the FRITZ!Box user interface to remove them safely and avoid any loss of data.

12.4 Accessing USB Memory

The participants in the home network have various possibilities for accessing the various storage media of the FRITZ!Box.

- Participants in the home network can use FTP software like FireFTP to exchange files among the FRITZ!Box storage media and workplaces.

Alternatively, you can enter <ftp://fritz.box> in the address line of your Internet browser to access the memory of the FRITZ!Box.

If you would like to use FTP software, see the documentation of the software as well as the instructions in the Online Help of the FRITZ!Box user interface.

- For access to media data like music, images and videos available on the memory or on storage media of the FRITZ!Box you can enable the FRITZ!Box media server. Suitable playback devices like TV sets, web radios, smartphones and the Windows Media Player can then call up the data for streaming from the media server.

Playback devices to be used in connection with the media server must support the UPnP AV standard.

Enable the “media server” function in the FRITZ!Box user interface under “Home Network / Storage (NAS) / Options Enabled”.

12.5 Sharing a USB Printer

You can connect a USB printer to the USB port of the FRITZ!Box to make it available to all participants in your home network. You can either release the printer for sharing as a network printer or use the FRITZ!Box USB remote connection software to connect it with a computer. Which option is preferable depends on how you intend to use the printer.

Using a USB Printer as a Network Printer

Configure the USB printer as a network printer on the FRITZ!Box if

- the participants in the home network are to be able to use the printer jointly and simultaneously.
- the printer is to be used by computers that use an operating system other than Windows (e.g. Mac OS X or Linux).

For information about how to configure a USB printer as a network printer, see the section [Setting Up a USB Printer as a Network Printer on page 74](#).

Using a USB Printer with FRITZ!Box USB Remote Connection

Configure the USB printer on the FRITZ!Box with the FRITZ!Box USB remote connection if

- the USB printer is an all-in-one device (fax/printer/scanner) and the entire range of functions is to be used.
- the USB printer is equipped with convenient features like ink level display and you would like to use these.
- the USB printer uses bidirectional data exchange. In other words: Not only does the computer send data to the printer, the printer also sends status messages to the computer. This communication in both directions is typical of the “Windows printers” or “GDI printers” that work only with special Windows device drivers.

For information about how to configure a USB printer with the USB Remote Connection, continue reading from the section [Configuring a USB Printer with FRITZ!Box USB Remote Connection on page 77](#).

Setting Up a USB Printer as a Network Printer

Work through the following steps to connect a USB printer to the FRITZ!Box and configure it for use as a network printer.

Preparing Configuration

1. Open the FRITZ!Box user interface.
2. Enable the Expert Mode.
3. Click “Home Network / USB Devices / USB Remote Connection”.
4. Make sure that the option “printers (including all-in-one printers)” is disabled.
5. Click “Apply”.
6. Connect the USB printer to the FRITZ!Box.

This concludes the preparations. Continue reading in the section for your operating system.

Setting Up a USB Printer in Windows 7, Vista and XP

1. Click “Start / Control Panel” and select the printer category of your operating system:
 - “Devices and Printers” (Windows 7)
 - “Printers” (Windows Vista)
 - “Printers and Faxes” (Window XP)
2. Click the printer icon with the right mouse button and select “Properties” or “Printer properties”.



If the printer is not displayed, you must first install the printer drivers for this device. Consult the documentation of your printer for instructions.

3. Switch to the “Ports” tab.
4. Click “Add” or “Add Port...”.
5. Double-click the “Standard TCP/IP Port” entry and click “New Port”, then “Next”.
6. Enter “fritz.box” in the “Printer Name or IP Address” field.



If the FRITZ!Box is configured as a WDS repeater or as an IP client, enter here the IP address at which the FRITZ!Box can be reached within the network.

7. Enter any name you wish in the “Port Name” field and click “Next”.
8. Select the “Custom” option and click “Settings...”.
9. Enable the “Raw” option.
10. Enter “9100” in the “Port Number” field and click “OK”.
11. Click “Next” and confirm with “Finish” and “Close”.
12. In the “[Printer name] Properties” window, switch to the “Ports” tab.
13. Disable the “Enable bidirectional support” option and click “Apply”.

The USB printer has been configured and can be used as a network printer.

Setting Up a USB Printer in Mac OS 10.5

1. Click in the dock on “System settings”.
2. Click “Print & Fax”.
3. Click the “+” sign.
4. Click “IP Printer”.
5. In the “Protocol” drop-down list, select the entry “HP Jet Direct – Socket”.
6. Enter “fritz.box” in the “Address:” input field.



If the FRITZ!Box is configured as a WDS repeater or as an IP client, enter here the IP address at which the FRITZ!Box can be reached within the network.

7. In the “Print Using:” drop-down list, select the printer that is connected to the USB port of your FRITZ!Box.



If the printer is not displayed, you must first install the printer drivers for this device. Consult the documentation of your printer for instructions.

8. Click “Add”.

The USB printer has been configured and can be used as a network printer.

Setting Up a USB Printer in Other Operating Systems



The names of entries or menus in other operating systems not described above may be slightly different than the terms we use here.

- As the port type, select “Raw TCP”.
- Enter “9100” as the port.
- As the printer name, enter “fritz.box”.



If the FRITZ!Box is configured as a WDS repeater or as an IP client, enter here the IP address at which the FRITZ!Box can be reached within the network.

Configuring a USB Printer with FRITZ!Box USB Remote Connection

If you are using an all-in-one device or would like to use the convenience features of a USB printer connected to the FRITZ!Box, we recommend installing the FRITZ!Box USB remote connection software. The FRITZ!Box USB remote connection program can be installed on computers with Windows 7, Vista or XP (32- and 64-bit).

Installing FRITZ!Box USB Remote Connection

Install the program for FRITZ!Box USB remote connection on all of the computers with which you want to use the connected USB device.

1. Connect the USB printer to the USB port of the FRITZ!Box.
2. Open the FRITZ!Box user interface.
3. Click “Expert Mode” and enable the expert settings.
4. Click “Home Network / USB Devices / USB Remote Connection”.
5. Enable “USB remote connection enabled”, then click the “USB remote connection software” link.
6. In the window “USB Remote Connection” click “Download”.
7. Download the file “fritzbox-usb-fernanschluss.exe”.
8. Double-click the file and follow the instructions on your screen.

The FRITZ!Box USB remote connection software is now installed on your computer. Repeat the steps in these instructions for all further Windows users who wish to use the USB remote connection on this computer.

Enabling the FRITZ!Box USB Remote Connection

1. Open the FRITZ!Box user interface.
2. Click “Expert Mode” and enable the expert settings.
3. Click “Home Network / USB Devices / USB Remote Connection”.
4. Enable the USB remote connection for printers and select the option “printers (including all-in-one printers)”.

For an all-in-one printer with a memory function, also enable the “USB storage media” option.

For an all-in-one printer with a scanner function, also enable the “Others (e.g. scanner)” option.

5. Click “Apply”.

The FRITZ!Box USB remote connection is enabled.

Using a USB Printer with FRITZ!Box USB Remote Connection

1. Open the FRITZ!Box USB remote connection by clicking the  icon in the Windows task bar.
2. Enter in the “My FRITZ!Box” area the FRITZ!Box password.
3. Click “Refresh”.
4. Click the USB printer in the “Devices” area.

The USB printer is being connected to the computer.



Do not conduct any firmware updates for USB devices that are connected with the computer via the FRITZ!Box USB remote connection.

13 Saving Energy with the FRITZ!Box

The FRITZ!Box combines a variety of devices in one device: VDSL and ADSL modem, WLAN router and media server. This means that you generally use much less power with the FRITZ!Box than you would with several separate devices.

What is more, the FRITZ!Box saves energy by reducing processing power on standby and lowering the power consumption of idle functions. The FRITZ!Box also offers various settings for energy-saving operation.

13.1 Saving Energy with the WLAN Radio Network

You can reduce the power consumption of the WLAN radio network by

- setting up night service for the WLAN radio network (see [page 45](#)).
- turning off the WLAN radio network with the “WLAN” button whenever no more WLAN devices are registered on the FRITZ!Box.
- enabling the setting “Automatically reduce transmitter power to the level actually needed”. This setting is configured in the “WLAN / Radio Channel” menu on the FRITZ!Box user interface.

13.2 Enabling Energy-saving Mode for USB Hard Drives

In the FRITZ!Box you can enable an energy-saving function for USB hard drives connected to the FRITZ!Box.

When the energy-saving function is enabled, connected USB hard drives will be switched off when they are idle—as long as the hard drives support the energy-saving function.

Enable the energy-saving function in the “Home Network / USB Devices” menu in the FRITZ!Box user interface. You can also test here, whether your USB hard disk supports the energy-saving function.

13.3 Saving Energy at the LAN Ports

For the individual LAN ports of your FRITZ!Box you can configure various operation modes. The power consumption of some modes is higher than others. Select the operation mode that is best suited to your needs in order to minimize the power consumption of the LAN ports.

The LAN ports can be configured in the FRITZ!Box user interface. In the “System / Energy Monitor” menu, the following operating modes are available on the “Settings” page:

Operating Mode	Functionality and Power Consumption
Always Enabled	The LAN port is always enabled. Highest power consumption.
Identify Automatically	The FRITZ!Box establishes LAN connections as needed. Lower power consumption than for the “Always Enabled” setting.
Disabled	The LAN port is disabled and consumes no power. The first LAN port cannot be disabled.

14 Help in Case of Errors

This chapter provides assistance if you are not able to open the user interface of your FRITZ!Box or are having problems with the DSL or WLAN connection.

For more comprehensive help, see the AVM knowledge database in the Internet, which can be accessed at the following address:

www.avm.de/en/service/FAQs

14.1 Cannot Establish a DSL Connection

The FRITZ!Box automatically establishes a connection to the DSL network as soon as it is connected with the DSL line. If the DSL connection is not established, check which kind (annex) of DSL is set in your FRITZ!Box and attempt to resolve the error.

Changing the Annex Setting of the FRITZ!Box

The FRITZ!Box cannot establish a connection to the DSL network. This is signaled by the continued flashing of the “Power” LED.

Cause

The kind of DSL (Annex A, B, J odr M) set in the FRITZ!Box is not the same as the annex used on your DSL line.

Help

1. Contact your Internet Service Provider to find out which annex is used on your DSL line.
2. Connect a computer with the FRITZ!Box either wirelessly via WLAN or using a network cable.
3. Open the FRITZ!Box user interface as described on [page 25](#).
4. Click the toolbar entry “Expert Mode” or in the “System / Expert Mode” menu to enable the expert settings of the FRITZ!Box and confirm your setting by clicking “Apply”.

5. Click “Internet / DSL Information” in the menu and select the “Line Settings” tab. In the “Annex Settings” section, make sure that the annex working on your DSL line is set. Save your settings by clicking “Apply”.

After the annex setting has been changed, the FRITZ!Box restarts automatically. The connection to the DSL network has been established as soon as the “Power” LED stops flashing and remains lit up.

14.2 The User Interface Does Not Open

If an error message is returned when you open the FRITZ!Box user interface, this can have various causes. Check the causes listed below and attempt to resolve the error.

Restarting the FRITZ!Box

The user interface cannot be opened or does not react.

Cause

Inconsistencies within the FRITZ!Box.

Help

1. Restart the FRITZ!Box.
Remove the power cable from the outlet.
 2. Wait about five seconds before reconnecting to the power supply.
 3. To make sure that the FRITZ!Box has finished restarting, wait until the “Power” LED lights up and stops flashing and, if you have switched on WLAN, the “WLAN” LED remains lit up as well. This ensures that the FRITZ!Box restart has been completed.
 4. Try again to open the FRITZ!Box user interface by entering fritz.box in the address field.
-

Checking the Cable Connections

The FRITZ!Box user interface is not displayed in your web browser.

Cause

The cable connections are not secure.

Help

Make sure that all cables are plugged in securely.

Checking Name Resolution

The user interface of the FRITZ!Box cannot be opened by entering [fritz.box](#).

Cause

The name resolution of the FRITZ!Box is not working.

Help

-
1. In the web browser, enter the following IP address in place of [fritz.box](#):
[192.168.178.1](#)
 2. If the user interface opens in response to this address, set the network adapters used to “Obtain the IP address automatically” (see [Obtaining an IP Address Automatically from page 66](#)).
-

Checking the IP Address

The user interface of the FRITZ!Box cannot be opened by a [fritz.box](#) nor by entering [192.168.178.1](#).

Cause

Incorrect IP address on the connected computer.

Help

Set the network adapter to DHCP so that the network address can obtain its IP address from the DHCP server of the FRITZ!Box. See the section [Obtaining an IP Address Automatically from page 66](#) for instructions.

If you still cannot open the user interface by entering fritz.box or by 192.168.178.1, use the fixed IP address of the FRITZ!Box as described on [page 87](#).

Disabling Dial-up Connections

The user interface is not opened; a window for a dial-up connection appears instead.

Cause

The browser must use the network connection between the computer and FRITZ!Box when the user interface is opened. For this the automatic establishment of a Dial-up Networking connection must be disabled.

Help

You can disable the automatic attempt to establish a Dial-up Networking connection. The following example explains how to check the settings of Internet Explorer 8:

1. Select the “Connections” settings page under “Tools / Internet Options”.
 2. In the “Dial-up and Virtual Private Network settings” section, enable the option “Never dial a connection”.
 3. As a final step, click “OK”.
-

Disabling Online Operation

The user interface does not appear in the window of your web browser.

Cause

The web browser is set for offline operation.

Help

Configure the web browser for online operation. Using the example of Internet Explorer 8:

1. Open the “Tools” menu.
2. If a checkmark is displayed in front of “Work Offline”, click this line.

The checkmark will be removed and Internet Explorer will switch to online operation.

Checking the Proxy Settings

The user interface does not appear in the window of your web browser.

Cause

The proxy settings of the web browser prevent the user interface from being opened.

Help

Enter the DNS name and the IP address of the FRITZ!Box as an exception in the proxy settings of the web browser, as described here for the example of the Internet Explorer 8.

1. Select the “Connections” settings page under “Tools / Internet Options”.
 2. Click the “LAN settings” button in the “Local Area Network (LAN) settings” area.
 3. In the “Proxy server” area of the next window, check the “Use a proxy server for your LAN” option and then click “Advanced”.
 4. Enter as “Exceptions”:
fritz.box; 192.168.178.1; 169.254.1.1
and click “OK”.
-

Checking the CGI Settings

The user interface does not appear in the window of your web browser.

Cause

The execution of CGI scripts is disabled in the web browser.

Help

Configure the web browser so that the execution of scripts is allowed in the user interface. Using the example of the Internet Explorer 8:

1. Select the “Security” settings page under “Tools / Internet Options”.
2. If the “Default level” button is not available for selection, the “Medium-high” security level is already configured, which means that CGI scripts can be executed in the Internet browser.
3. Proceed as follows if the “Default level” button is available for selection:
4. Select the “Local intranet” icon and click the “Sites” button.
5. In the next window, click the “Advanced” button and enter in the “Add this website to the zone:” field:

fritz.box

Click “Add”.

6. Disable the “Require server verification (https:) for all sites in this zone” option and click “Close”.
-

Checking Security Software

The user interface cannot be displayed in the web browser.

Cause

Security software is blocking access to the user interface.

Help

Security software like firewalls can prevent access to the user interface of the FRITZ!Box. Configure exceptions for the FRITZ!Box in all of the enabled security software.



If you would like to exit security software to test access to the FRITZ!Box, remove the DSL cable first. After testing, first start the security software before reinserting the DSL cable and connecting to the Internet!

Opening the User Interface of the FRITZ!Box

The FRITZ!Box is equipped with a fixed IP address that cannot be changed. The FRITZ!Box always can be reached at this IP address. This fixed IP address is:

Fixed IP address	169.254.1.1
------------------	-------------

Proceed as follows to open the FRITZ!Box user interface using this IP address:

1. Connect the FRITZ!Box to the computer using the network cable (yellow). For more information, see the section [Connecting Computers to the LAN Port from page 17](#).
2. Make sure that the computer obtains its IP address automatically. You can check this setting in the computer's IP settings (see section [Obtaining an IP Address Automatically from page 66](#)).
3. Restart your computer.
4. Start your Internet browser and enter the FRITZ!Box's fixed IP address:

169.254.1.1

The FRITZ!Box user interface opens.



Once you have reached the FRITZ!Box user interface again, you should check the FRITZ!Box settings and correct them if necessary.

14.3 Cannot Establish a WLAN Connection

If you are not able to establish a WLAN connection between your computer and the FRITZ!Box, then please undertake the following measures to seek the source of the error and resolve it.

Enabling the WLAN Device

The WLAN device cannot find a wireless network.

Cause

The WLAN device is not ready for operation.

Help

Make sure that the WLAN device is ready for operation. Some of the WLAN devices installed in notebooks must be activated by flipping a switch on the notebook.



For questions on the WLAN device of your computer, please contact the manufacturer.

Enabling WLAN

The wireless network of the FRITZ!Box is not found by the WLAN device.

Cause

WLAN is not enabled in the FRITZ!Box. If the “WLAN” LED on the FRITZ!Box is not lit up or is flashing, this means that WLAN is not enabled.

Help

Press the WLAN button on the FRITZ!Box. The “WLAN” LED begins flashing and then lights constantly. This means that the WLAN function is enabled.

Announcing the Name of the Radio Network

The WLAN device cannot find the wireless network of the FRITZ!Box.

Cause

The name of the wireless network of the FRITZ!Box is concealed.

Help

In the WLAN settings of the FRITZ!Box, enable the “Name of the radio network visible” option.

1. Connect the FRITZ!Box to a computer using a network cable, as described in the section [Connecting Computers to the LAN Port on page 17](#).
 2. Start a web browser.
 3. Enter fritz.box in the address field.
 4. In the “Interfaces” area on the “Overview” page, select “WLAN”, or open the “WLAN” menu in the navigation bar on the left.
 5. In the “Radio Network” page, enable the option “Name of the radio network visible”.
 6. Click the “Apply” button at the bottom of the page.
 7. Remove the network cable and try again to establish a connection via WLAN.
-

Comparing the Security Settings for WLAN

Make sure that the WLAN security settings registered in the FRITZ!Box agree with the security settings of the WLAN adapter.

Here is how to view the WLAN security settings of the FRITZ!Box and print them out.

1. Connect the FRITZ!Box to a computer using a network cable. Proceed as described in the section [Connecting Computers to the LAN Port from page 17](#).
2. Start a web browser.

3. Enter fritz.box in the address field.
4. In the “Interfaces” area on the “Overview” page, select “WLAN”, or select the “WLAN” menu in the navigation bar on the left.
5. Open the “WLAN / Security” menu.
6. Click the “Apply” button.

A window with the WLAN security settings will be displayed. Print out the page by clicking the “Print Page” button.
7. Remove the network cable and check the configuration of the WLAN adapter in the printout. Try again to establish a connection.

Testing the WLAN Connection Without Security Settings

Disable the WLAN security settings to test whether a WLAN connection between the FRITZ!Box and the WLAN device is possible at all.

1. Connect the FRITZ!Box to a computer using a network cable. Proceed as described in the section [Connecting Computers to the LAN Port from page 17](#).
2. Open the user interface of the FRITZ!Box in a web browser. Proceed as described in the section [Opening the User Interface on page 25](#).
3. In the “Interfaces” area on the “Overview” page, select “WLAN”, or open the “WLAN” menu in the navigation bar on the left.
4. Click the “WLAN / Security” menu and enable the option “non-encrypted”.
5. Then click the “Apply” button.
6. Remove the network cable and try again to establish a connection.



This non-secured condition should be used only for testing, to find out whether a WLAN connection is possible at all.

If the attempt to connect to the WLAN using the non-encrypted connection is not successful either, check the installation of the WLAN device and contact the manufacturer of the WLAN device if necessary.

Enable WLAN encryption again after completing the tests. Follow the steps listed above and then enable the kind of encryption that was previously configured.

Installing the Current Service Pack

The WLAN connection to the FRITZ!Box cannot be established using the Microsoft WLAN Service (WZC: Windows Zero Configuration) in Windows XP with Service Pack 2.

Cause

The required Microsoft patch for WPA2 (IEEE 802.11i) may not be installed.

Help

Install Service Pack 3 (SP3) for Windows XP, available as a free download from Microsoft. Then Microsoft WLAN Service will support WPA2, so that a WLAN connection can be established to the FRITZ!Box.

Avoiding WLAN Channels with DFS

The FRITZ!Box loses the WLAN connection in the 5-GHz frequency band for no apparent reason.

Cause

A forced channel change is taking place. In the 5-GHz frequency band the WLAN base station is programmed to change the channel whenever a radar source transmits on the same channel (Dynamic Frequency Selection, DFS).

Help

You can prevent forced channel changes by selecting in the FRITZ!Box a channel for the 5-GHz frequency band that does not use DFS (channels 36, 40, 44, 48).

Ruling Out Interference Caused by Other Wireless Networks

If there are other devices in the immediate vicinity of your FRITZ!Box that use the same frequency band, simultaneous use of frequencies can result in mutual interference (for example, fluctuations or interrupted connections). Disruptions can be caused by other WLAN base stations, but also by devices like baby monitors, game consoles, garage door openers, Bluetooth devices, or wireless AV bridges, which also use the 2.4-GHz frequency band. In this case, please test a different radio channel for your FRITZ!Box.

Alternatively, you can set the radio channel to “Autochannel”. This enables the autochannel function, so that the FRITZ!Box searches for the best WLAN channel itself.

For applications that rely on a steady, high throughput rate (“streaming”), you should use the 5-GHz frequency band. This radio band provides more channels and is subject to significantly less external interference.

To set the radio channel in the user interface, your computer must be connected with the FRITZ!Box by network cable or wirelessly. If your computer is connected via WLAN, continue with Step 2 of the instructions below. In this case, note that the existing WLAN connection is interrupted as soon as you apply the changed settings. Afterward you have to reconnect your computer with the FRITZ!Box.

1. Connect the FRITZ!Box to a computer using a network cable. Proceed as described in the section [Connecting Computers to the LAN Port from page 17](#).
2. Start a web browser.
3. Enter fritz.box in the address field.
4. Open the “WLAN / Radio Channel” menu in the navigation bar on the left.
5. You may have to enable the “Adjust radio channel settings” option.
6. Select a different radio channel from the “Radio channel” list.

7. Click the “Apply” button.
8. Remove the network cable and check whether interference continues to occur.

15 Taking the FRITZ!Box out of Operation

In this chapter you receive tips and recommendations for taking the FRITZ!Box out of operation.



Please also follow our instructions for the correct disposal of waste equipment on [page 109](#).

15.1 Restoring the FRITZ!Box Factory Settings

Restore the factory settings of the FRITZ!Box. This is strongly recommended if you are planning to pass the FRITZ!Box on to another user.

Resetting the FRITZ!Box has the following effects:

- All settings you made in the FRITZ!Box are then deleted.
- The factory settings' WLAN key will be activated again.
- The IP configuration of the factory settings will be re-stored.

Restoring Factory Settings

1. In the FRITZ!Box user interface, select the “System / Reset” menu.
2. On the “Factory Settings” page, click the “Load Factory Settings” button.

The FRITZ!Box is reset to its factory settings.

15.2 Uninstalling Software

Additional software for the FRITZ!Box is available on the web pages of AVM at www.avm.de/en/download.

If you have installed supplementary programs on one or more computers, uninstall the software using the control panel of your Windows operating system.

Uninstalling Software in Windows 7

1. Open “Start / Control Panel / Programs”.
2. Under “Programs and Features”, click “Uninstall a program”.
3. Select in the list the AVM software to be uninstalled.
4. Click the “Uninstall/Change” button.

The software will be uninstalled.

Uninstalling Software in Windows Vista

1. Open “Start / Settings / Control Panel / Programs and Functions”.
2. Select in the list the AVM software to be uninstalled.
3. Click the “Uninstall/Change” button and confirm with “Continue”.

The software will be uninstalled.

Uninstalling Software in Windows XP

1. Open “start / Control Panel / Add or Remove Programs”. Make sure that the “Change or Remove Programs” button is selected in the column at left.
2. Select the AVM software to be uninstalled from the list of “Currently installed programs”.
3. Click the “Change/Remove” button.

The software will be uninstalled.

16 Technical Specifications

16.1 Ports and Interfaces

- DSL modem in accordance with standard ITU G.992.1 Annex A and B (G.dmt), ITU G.992.3 Annex A and B (ADSL2), ITU G.992.5 Annex A and B (ADSL2+), ITU G.992.3/5 Annex M, ITU G.992.3/5 Annex J, ITU G.994.1 (G.hs)
- Four LAN ports via RJ45 sockets (standard Ethernet, 10/100 base-T)
- One USB host controller (USB version 2.0)
- WLAN base station with support for wireless networks
 - IEEE 802.11a – 54 Mbit/s
 - IEEE 802.11b – 11 Mbit/s
 - IEEE 802.11g – 54 Mbit/s
 - IEEE 802.11n – 300 Mbit/s

16.2 Router Functions

- Router
- DHCP server
- Firewall with IP masquerading/NAT
- IPv4 and IPv6
- Child protection and filter lists
- Port forwarding
- Dynamic DNS
- VPN

16.3 User Interface and Display

- Settings and status messages via a web browser on a connected computer
- Five LEDs indicate the condition of the device

16.4 Physical Specifications

- Dimensions (W x D x H): approx. 210 x 155 x 25 mm
- Supply voltage: 230 V / 50 Hz
- Maximum power consumption: 12 W
- Firmware can be updated
- Conform to CE standards
- Ambient conditions
 - operating temperature: 0°C – +40°C
 - storage temperature: -20°C – +70°C
 - relative humidity (operation): 10% – 90%
 - relative humidity (idle): 5% – 95%

16.5 Cable

Network Cable

The network cable (yellow) of the FRITZ!Box 3270 is a standard category 5 (Cat 5) Ethernet cable. Please use a standard STP-type (Shielded Twisted Pair) Ethernet cable of category 5 (Cat 5) to replace or extend the Ethernet cable. To extend the cable you will need a shielded RJ45 double coupling (Cat 5) with a 1:1 pin assignment. You can use both straight cables and crosslink cables. All components are available from specialized vendors.

When components of a category smaller than Cat 5 are used, reduced transmission rates may result.

AVM recommends using a network cable no more than 100 meters long.

17 Customer Service

Be it product documentation, frequently asked questions (FAQs) or support: this chapter presents information on all important service topics.

17.1 Documentation on the FRITZ!Box

To take advantage of all commands and features of your FRITZ!Box, consult the following documentation:

Help

In the FRITZ!Box user interface you can open the comprehensive Help by clicking the “Help” icon and the “Help” buttons.

Manual

The PDF file of the manual can be opened and downloaded from the Internet at the following address:

www.avm.de/en/service/manuals

Choose the “FRITZ!Box” product group and then your “FRITZ!Box 3270”. The PDF is opened.



The current Adobe Acrobat Reader for reading PDF documents can be downloaded from the Internet free of charge at www.adobe.com.

17.2 Information in the Internet

On its web site AVM presents comprehensive information on your AVM product.

Videos on the FRITZ!Box

Videos on many of the FRITZ!Box functions are available, showing animated demonstrations of how to set up the individual functions.

The videos can be viewed at the following address:

www.avm.de/en/service/FRITZ_Clips

Frequently Asked Questions (FAQs)

We would like to make our products as easy to use as possible. If you still have problems, sometimes you need just a tip to resolve them.

In our FAQs you will find answers to the questions users ask about our products most often. The FAQs can be viewed at the following address:

www.avm.de/en/service/FAQs

17.3 Support from the Support Team

Should problems with your FRITZ!Box arise, we recommend taking the following steps:

1. If you have questions about starting operation of your FRITZ!Box, please consult the following chapters again:
 - [Before You Connect the FRITZ!Box from page 12](#)
 - [Connecting the FRITZ!Box from page 15](#)
 - [Connecting the Computer to the FRITZ!Box from page 17](#)
2. If you have any problems, seek first aid by consulting the chapter [Help in Case of Errors from page 81](#).

This chapter also presents tips on problems with establishing connections.

3. Read our FAQs in the Internet.

www.avm.de/en/service/FAQs

This site contains answers to questions our customers have frequently asked our Support team.



Please take advantage of the information sources described above before contacting AVM support.

Support by E-mail

You can send us an English-language e-mail request at any time using the “Service” area of our web site. The “Service” area can be reached at:

www.avm.de/en/service

1. Select the product for which you need support from the “Support” area.
2. Click the “Mail Form” link to open the e-mail form.
3. Fill out the form in English.
4. Send it to AVM by clicking the “Send” button.

Our Support team will respond by e-mail as quickly as possible.

17.4 Manufacturer's Warranty

We offer a manufacturer's warranty of 5 years on the hardware of this original product. The warranty period begins with the purchase date from the first end user. Compliance with the warranty period can be proven by submission of the original invoice or comparable documents. This warranty does not restrict your warranty rights based on the contract of sale or other statutory rights.

We will remove defects to the product which are demonstrably due to faults in materials or manufacturing. Our warranty does not cover defects which occur due to incorrect installation, improper use, non-observance of instructions in the user manual, normal wear and tear or defects in the environment of the system (third-party hardware or software). We may, at our discretion, repair or replace the defective product. Claims other than the right to the removal of defects which is mentioned in these terms of warranty are not constituted.

We guarantee that the software conforms with general specifications, not, however, that the software meets your individual requirements. Delivery costs will not be reimbursed. Products which have been replaced revert to our ownership. Claims recognized under warranty entail neither an extension

or recommencement of the warranty period. If we reject a warranty claim, this claim lapses no later than six months after being rejected by us.

This warranty shall be governed by German substantive law, to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG).

18 AVM Products for the FRITZ!Box

Here we introduce additional devices by AVM that are designed to be used in combination with your FRITZ!Box 3270.

FRITZ!Powerline 500E



With FRITZ!Powerline 500E your electrical outlet is transformed into a secure network line. Just connect your devices over the power line—without installing any cables:

- Networks FRITZ!Powerline 500E, computer, printer, TV, stereo, game console, media player and other network devices
- Especially suitable for broadband-intensive applications like streaming, surfing, gaming, Internet TV, video on demand and VoIP
- Throughput of up to 500 Mbit/s over a range of up to 500 meter over your own power mains
- Low operating power consumption, under 1 W on standby
- Encrypted securely upon delivery with 128-bit AES
- Immediately operational at every outlet
- Immediately ready for operation without any new software
- Available in a practical set with two adapters; additional adapters can be networked easily and securely at the touch of a button.

FRITZ!WLAN USB Stick N



Up to 300 Mbit/s

Dual band

WPA2 (802.11i)

Stick & Surf

FRITZ!WLAN USB Stick N connects your computer easily and safely with your FRITZ!Box WLAN and other compatible WLAN routers:

- USB stick for WLAN N with up to 300 Mbit/s
- WLAN support for either 2.4-GHz or 5-GHz connections (dual band)
- Supports the conventional standards 802.11n/g/b/a
- WPA2 encryption for maximum WLAN security (802.11i)
- Stick & Surf: secure wireless network without configuration
- Supports WPS for easy, fast configuration of secure WLAN connections

For more information, see www.avm.de/en/Produkte/FRITZ_WLAN/FRITZ_WLAN_USB_Stick_N.

FRITZ!WLAN USB Stick



Up to 150 Mbit/s

WPA2 (802.11i)

Stick & Surf

FRITZ!WLAN USB Stick connects your computer easily and safely with any WLAN router:

- USB stick for WLAN N with up to 150 Mbit/s
- Also supports the WLAN standards 802.11g and b
- WLAN support for 2.4-GHz connections
- WPA2 encryption for maximum WLAN security (802.11i)
- Stick & Surf: secure wireless network without configuration
- Supports WPS for easy, fast configuration of secure WLAN connections

For more information, see www.avm.de/en/Produkte/FRITZ_WLAN/FRITZ_WLAN_USB_Stick.

FRITZ!WLAN Repeater N/G



Up to 300 Mbit/s

WPS

Media function

With the FRITZ!WLAN Repeater N/G the range of the wireless network can be extended quickly and easily:

- Compatible with all conventional WLAN routers (802.11n/g/b/a radio standards)
- WLAN support for either 2.4-GHz or 5-GHz connections (dual band)
- Simple configuration at the click of a button via WPS, using a Wizard or manually
- Media function: integrated audio output and miniature FM transmitter for transferring music or web radio to stereo/radio

For more information, see www.avm.de/en/Produkte/FRITZ_WLAN/FRITZ_WLAN_Repeater_N_G.

FRITZ!WLAN Repeater 300E



Up to 300 Mbit/s

WPS

Gigabit LAN

With the FRITZ!WLAN Repeater 300E the range of the wireless network can be conveniently extended:

- Compatible with all conventional WLAN routers (802.11n/g/b/a radio standards)
- WLAN support for either 2.4-GHz or 5-GHz connections (dual band)
- Simple configuration at the click of a button via WPS, using a Wizard or manually
- Integrated gigabit LAN interface provides for simple integration of network devices into the home network or the Internet

For more information, see www.avm.de/en/Produkte/FRITZ_WLAN/FRITZ_WLAN_Repeater_300E.

Legal Notice

Legal Notice

This documentation and the software it describes are protected by copyright. AVM grants the non-exclusive right to use the software, which is supplied exclusively in object code format. The licensee may create only one copy of the software, which may be used exclusively for backup use.

AVM reserves all rights that are not expressly granted to the licensee. Without previous approval in writing, and except for in cases permitted by law, it is particularly prohibited to

- copy, propagate or in any other manner make this documentation or this software publicly accessible, or
- process, disassemble, reverse engineer, translate, decompile or in any other manner open the software and subsequently copy, propagate or make the software publicly accessible in any other manner.

The licensing conditions are presented in the FRITZ!Box 3270 user interface under the “Legal Notice” heading.

This documentation and software have been produced with all due care and checked for correctness in accordance with the best available technology. AVM GmbH disclaims all liability and warranties, whether express or implied, relating to the AVM product's quality, performance or suitability for any given purpose which deviates from the performance specifications contained in the product description. The licensee bears all risk in regard to hazards and impairments of quality which may arise in connection with the use of this product.

AVM will not be liable for damages arising directly or indirectly from the use of the manual or the software, nor for incidental or consequential damages, except in case of intent or gross negligence. AVM expressly disclaims all liability for the loss of or damage to hardware or software or data as a result of direct or indirect errors or destruction and for any costs (including connection charges) related to the documentation and the software and due to incorrect installations not performed by AVM itself.

The information in this documentation and the software are subject to change without notice for the purpose of technical improvement.

© AVM GmbH 2012. All rights reserved. Documentation release 03/2012

AVM Audiovisuelles Marketing
und Computersysteme GmbH
Alt-Moabit 95
10559 Berlin
Germany

AVM Computersysteme
Vertriebs GmbH
Alt-Moabit 95
10559 Berlin
Germany

AVM in the Internet:
www.avm.de/en

Marks: Marks like AVM, FRITZ! and FRITZ!Box (product names and logos) are protected marks owned by AVM GmbH. Microsoft, Windows and the Windows logo are trademarks owned by Microsoft Corporation in the USA and/or other countries. Apple, App Store, iPhone, iPod and iPad are marks owned by Apple Inc. in the USA and/or other countries. IOS is a mark owned by Cisco Technology Inc. in den USA and/or other countries. Google and Android are marks owned by Google Inc. in the USA and/or other countries. All other marks (like product names, logos, commercial names) are owned by their respective holders.

Declaration of CE Conformity

The manufacturer AVM GmbH
Alt-Moabit 95
10559 Berlin

herewith declares that the product

FRITZ!Box 3270
ADSL WLAN router

complies with the following directives:

1999/5/EC	R&TTE Directive: Radio Equipment and Telecommunications Terminal Equipment
2009/125/EC	EU directive: ecodesign requirements for energy-related products

The following norms were consulted to assess conformity:

- EN 60950-1:2006 + A11: 2009 + A1: 2011	- EN 300 328 V1.7.1 - EN 301 893 V1.6.1
- EN 55024: 2010	- EN 50371:2002
- EN 301 489-1 V1.8.1	
- EN 301 489-17 V2.1.1	



The CE symbol confirms that this product conforms with the above mentioned norms and regulations.

A handwritten signature in blue ink, which appears to read 'P. Fixel', is positioned above the printed name of the Technical Director.

Berlin, 2012.02.15

Peter Fixel, Technical Director

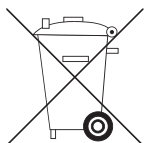
Indication of Countries

The WLAN radio technology of this device is designed for use in all countries of the European Union and in Switzerland, Norway and Iceland. In France only indoor operation is permitted.

Disposal Information

In accordance with European regulations and the Waste Electrical and Electronic Equipment Act (WEEE), the FRITZ!Box 3270, as well as all devices and electronic components contained in the package, may **not** be disposed with household waste.

Please bring these to a collection point in your local community for the disposal of electric and electronic appliances.



Symbol for labeling electrical and electronic scrap



Watch for the symbol designating electrical and electronic scrap. Electrical and electronic equipment must be disposed of separately from household waste.

Drilling Template

See the next page for a drilling template. Use the drilling template as a guide to mark the holes needed to mount the FRITZ!Box on a wall.



Be sure to print out the page with the drilling template in its original size, or 100%. Do not enlarge it, adjust its size, reformat or rescale it in your printer settings.



Glossary

ADSL

short for Asymmetric Digital Subscriber Line

ADSL (G.992.1/G992.2) was developed on the basis of DSL technology in order to satisfy the increasing demand for higher throughput rates during uploading and downloading.

Designates a fast kind of data transmission that works with standard copper cables and transports signals in both directions at different speeds (upstream at 640 Kbit/s and downstream at up to 9 Mbit/s).

ADSL2

short for Asymmetric Digital Subscriber Line 2

ADSL2 (G.992.3) is a further development of the ADSL standard.

ADSL2 offers range much greater than did the first ADSL generation, and is significantly more robust than ADSL, as it can simply disable single carrier frequencies when they produce interference. This feature allows ADSL2 to prevent synchronization losses.

With a throughput rate of up to 12 Mbit/s downstream, ADSL2 offers considerably greater bandwidth than ADSL.

ADSL2 is completely downward compatible, meaning that terminal devices compliant with ADSL can also be operated on ADSL2 lines, although they cannot exploit the advantages of ADSL2.

In practice ADSL2 has become less important since the ADSL2+ standard has made higher throughput rates possible.

ADSL2+

short for Asymmetric Digital Subscriber Line 2 with extended bandwidth

ADSL 2+ (G.992.5) is a further development of the ADSL standard.

ADSL2+ offers a doubled frequency range used for downstream transmission, and thus double the maximum bandwidth achievable for downstream to 24 Mbit/s.

ADSL2+ is completely downward compatible, meaning that terminal devices compliant with ADSL and ADSL2 can also be operated on ADSL2+ lines, although they cannot exploit the advantages of ADSL2+.

cable modem

A cable modem is a device that transmits data over cable television networks. It is used to integrate broadband Internet connections over cable connections (cable Internet). The cable modem is located between the cable connection and the Internet router at the customer's premises. The computer is connected either via LAN or the USB port. Some cable modems are combined with a WLAN access point that establishes a radio connection to the computer.

DDNS

short for Dynamic Domain Name System

DDNS is a service which allows a computer always to be reached under the same domain name despite constantly changing public IP addresses. This means the home network can always be reached from the Internet, regardless of the user's location. Even private users have an economical way of placing their own Internet offers on their computer at home.

Every time the Internet connection is established, the Internet Service Provider assigns a new public IP address.

Each time the IP address changes, the current IP address is transmitted to a special DDNS server. Except for the few seconds between the cancellation of the old IP address and the notification of the new IP address, the computer can always be reached at the selected domain name.

default gateway

gateway ([see glossary](#))

DHCP

short for Dynamic Host Configuration Protocol

DHCP is a protocol for dynamically negotiating the operating parameters of the TCP/IP protocol ([see glossary](#)). The computers in a local IP network (DHCP clients) access the DHCP server as part of their operating systems' start procedure.

The central administration of the TCP/IP operation parameters makes it possible to avoid address conflicts caused by IP addresses ([see glossary](#)) accidentally assigned more than once.

DHCP is used in IPv4 networks ([see glossary](#)).

DHCP server

The DHCP server assigns each client an IP address that is has not yet been assigned at the present time. The DHCP server also informs the client of the IP addresses of the DNS server to be used and of the default gateway. In assigning the IP addresses the DHCP server selects from a prescribed range of IP addresses.

DHCP is used in IPv4 networks ([see glossary](#)).

DNS

short for Domain Name System

Domain Name Service takes care of determining the IP address for a given domain name. This Domain Name Service runs on every computer. It accepts the domain name entered by a user and inquires about the corresponding IP address at a DNS server known to the service. If a DNS server cannot answer the inquiry itself, it can inquire about the IP address (DNS resolution) at other DNS servers.

If the Domain Name Service receives negative information from the DNS server (domain name not known), it can send inquiries to other DNS servers it knows or return a corresponding error message to the user. If it receives the desired IP address instead, the application can use the IP address to retrieve the destination desired by the user.

This hierarchical system of DNS servers is known as the Domain Name System. The addresses of the DNS servers at which the Domain Name Service is to inquire by default generally are handed over to the computer by the Internet Service Provider automatically whenever a connection to the Internet is established.

download

Download designates the transfer of files from the Internet to a computer.

DSL modem

A DSL modem connects a computer to the Internet via the DSL line. In contrast to the analog modem, a connection via the DSL modem does not mean that the telephone line is busy.

DSL router

A DSL router generally combines three different devices: a DSL modem ([see glossary](#)), a router, and a LAN switch.

A DSL router serves, first, to connect multiple computers or other network devices together to form a local network (LAN) so that the devices can exchange data with each other.

Second, a DSL router provides a central Internet connection that can be used by all devices in the home network at the same time. The DSL router's job is to control the data traffic between the local network and the Internet. If the DSL router is equipped with a firewall ([see glossary](#)), it protects the devices in the home network against attacks from the Internet.

DSL splitter

A DSL splitter is a device that separates telephone and DSL signals.

You need a DSL splitter if you have a fixed line and a DSL line. The splitter separates the telephone and DSL signals, which use the same cable to access your house or apartment. The

splitter conducts telephone signals to your analog telephones or to the NT. DSL signals are sent on to the DSL modem or DSL router.

dynamic IP address

A dynamic IP address is an IP address valid only for the duration of one Internet or network session.

Every computer participating in the Internet must have a uniquely assigned public IP address. Since only a limited number of such IP addresses is available, they must be used sparingly. That is why most of the Internet participants who dial in to the Internet receive a dynamic IP address. They are called dynamic because every participant receives a new public address that has not been assigned yet each time she or he dials in to the Internet.

By contrast, dynamic addresses are usually used in local IP networks because they are easy to handle, and because using them avoids incorrect IP address entries or unintentional double assignments.

file system

A file system saves and manages files on a data medium (for instance, a hard drive or flash drive). The way the files are stored varies from one file system to the next.

The different operating systems offer different file systems. In Windows 7, Windows Vista and Windows XP the file systems FAT32 and NTFS are used most frequently. The file system of a data storage medium can be changed, for instance from FAT32 to NTFS.

firewall

A firewall protects a computer or local network against attacks from the Internet.

Most firewalls work with packet filters, which merely check the IP addresses and port numbers of incoming and outgoing data packets and filter the packets according to prescribed rules.

Within IPv4 networks, some firewalls also integrate additional concepts like IP masquerading and NAT to decouple data traffic by distinguishing strictly between the internal and external network.

Especially effective firewalls go even further, analyzing and evaluating the contents of the packets and filtering them according to prescribed rules. Such techniques may also include a Stateful Packet Inspection Firewall, for instance.

firmware

The firmware is the software of an electronic device, which is stored in the device and controls its functions.

fixed IP address

Fixed IP addresses are IP addresses ([see glossary](#)) which are permanently assigned to a computer or another device like a network printer.

Assigning fixed IP addresses makes sense in cases where a computer is always supposed to be accessible at a certain address (for instance, a web server or an e-mail server).

FTP

short for File Transfer Protocol

The File Transfer Protocol allows files to be exchanged between two computers in the Internet. A computer on which the files are made available for downloading is called an “FTP server”. A special program is required for downloading files, known as an “FTP client”. Some web browsers contain FTP clients, but they are also available as independent software.

gateway

Gateway is a general term designating an interface between two networks. Such a network interface can be realized using a router or a bridge, for instance.

If a computer wants to transfer data packets to a computer in another network, it must first transmit the packet to the gateway. To do this, the computer must know the address of the gateway.

If all packets that cannot be delivered in a local network always are to be transmitted to their given recipients via the same gateway, for this purpose the address of the gateway must be saved as the default gateway in the network settings of the computer.

Such a default gateway for the computer is negotiated automatically by the operating system or the dialing software whenever an ISDN-Controller or ADSL-Controller establishes a connection to the Internet.

If a router is used for the shared Internet access in a local network, the IP address of the router must be entered as the default gateway in the TCP/IP settings of each computer that wishes to use the Internet connection.

HSPA

short for High Speed Packet Access

HSPA is a third-generation mobile radio standard further developed from the the UMTS mobile radio standard. HSPA provides for throughput rates in the mobile radio network that are comparable with DSL (3.6 to 13.98 Mbit/s).

hub

A hub is a device that is used to connect network devices to each other, for instance through an Ethernet. Network devices are connected to each other in a star network, with each network device connected to the hub. There are no direct connections between the network devices.

A hub can either send or receive data. Received data are sent to all connected devices. All connected devices share the data throughput.

Internet telephony

VoIP ([see glossary](#))

IP

short for Internet Protocol

The IP Internet Protocol is the most important basic protocol for the control of data exchange in local networks and in the Internet. The Internet protocol works without a connection; in other words, data packets are transmitted from the sender to the recipient without previous consultation. The addresses of the recipient and the sender in the data packets are given as IP addresses.

IP address

In IP-based networks, for instance in the Internet and local networks, all connected devices are addressed via their IP addresses. So that data packets are sure to be delivered to the right address, each IP address may be assigned only once within the Internet or a local IP network.

IPv6 addresses are structured differently from IPv4 addresses. IP addresses can be written in decimal, octal or hexadecimal format.

IP masquerading

IP masquerading is a technique used within IPv4 networks. With IP masquerading a computer or LAN can be protected from unauthorized connection requests from the Internet. Masquerading works by converting the IP addresses used in a network to one public IP address. From the outside it appears as if all requests are sent from a single computer.

IP network

A network in which data exchange takes place on the basis of the Internet Protocol (IP) is called an IP network.

IPv4

short for Internet Protocol version 4

IPv4 is currently the conventional Internet protocol.

IPv4 addresses are 32 bits long, such that IPv4 offers an address space of 2^{32} IP addresses, or just over four billion. The latest estimates suggest that the last IPv4 addresses will be assigned by the beginning of 2012.

The successor protocol to IPv4 is IPv6.

IPv6

short for Internet Protocol version 6

The successor protocol to IPv4 is IPv6.

IPv6 addresses are 128 bits long. This means that IPv6 makes approximately 340 undecillion ($\sim 3.4 \times 10^{36}$) IPv6 addresses available. Each private user can be allotted over 18 quintillion public IPv6 addresses from her or his Internet Service Provider.

The dearth of addresses in IPv4 is only one of the reasons for introducing IPv6. IPv6 also offers additional advantageous characteristics in the framework of communication within IP networks.

NAS functionality

NAS is short for Network Attached Storage

NAS designates one or more devices that are integrated into a network to provide storage space.

In connection with the FRITZ!Box, NAS functionality means that various services for connected USB storage media are available in the FRITZ!Box so that it is easier for you to use your data and make them available in the local network. It is easy to exchange documents in the local network via the storage medium on the FRITZ!Box. The media server makes music, images and videos in the network available to compatible playback devices. Files can also be released for sharing in the Internet, and local memory expanded by adding online storage.

NAT

short for Network Address Translation

NAT is a technique used within IPv4 networks. NAT is used in routers to replace the address information in data packets with new address information. A typical application for NAT is routers that connect local networks with the Internet. In local networks, every network device has a private IP address, while generally there is only one public IP address available for the Internet. To grant the network devices access to the Internet, the router replaces the private IP address of the sender with its own public IP address in all outgoing data packets. The router saves all necessary information in a table so that incoming data packets can then be assigned to the correct network device.

port

So that a single network connection on a computer can be used by multiple applications to exchange data with remote sites at the same time, a computer administers what are known as ports for the IP-based protocols TCP and UDP. Ports substantiate the point of access for the data packets delivered via the IP Internet protocol. While the IP address determines the destination computer quite generally, the port addresses the communication interface provided by an application for a certain communication procedure.

The Internet protocol allots 16 bits for the specification of the port number. Thus a total of 65,535 different port numbers can be specified. Ports up to port number 1,024 are reserved for special system applications and typical Internet applications. These include, for instance, the port numbers 21 for FTP (File Transfer Protocol), 25 for SMTP (Simple Mail Transfer Protocol), 53 for DNS (Domain Name Service) and 80 for HTTP (Hypertext Transfer Protocol).

Ports are primarily of interest to users for their role in protecting an Internet connection from external attacks. Most firewalls offer the possibility of preventing data traffic on certain ports. This means that certain port numbers can be blocked to prevent data from being delivered to system services. This

is also a way of preventing any Trojans (malicious applications opening backdoors on computers) that may have infected your computer from receiving data on ports it created as means of accessing your computer for potentially damaging activities. A firewall blocks most of the atypical port numbers not required for normal operation of an application and offers specialized users the opportunity to forward specified ports.

port forwarding

With port forwarding it is possible to specify ports that will allow all incoming or outgoing data packets to pass through a router or firewall.

If a computer from the local network offers server services, for instance, the settings of a router using NAT ([see glossary](#)) or IP masquerading ([see glossary](#)) must enable or forward the port used by the server service for access to incoming data packets and thus keep it open permanently. The private IP address of the given computer must be saved as the destination address for all of the packets arriving at the port.

Typical server applications that require port forwarding are FTP and web servers. To allow access to a computer via remote management software like Symantec pcAnywhere or Microsoft's Remote Desktop, or even use of a file-sharing program like eDonkey, the required ports must be released for port forwarding. Port forwarding settings for the most important application cases are quite simple as long as the settings of the router or the firewall already contain rules with a corresponding preconfiguration.

private IP address

Private IP addresses are used for computers and other network devices within local IPv4 networks.

Since many local IP networks are not connected to the Internet except via single computers or routers (gateway), certain address ranges are excluded from the publicly available IP addresses so that they are available for assignment in local IP

networks. An IP address may only be assigned once within the local network. A private IP address may exist in any number of other local networks.

public IP address

A public IP address is an IP address ([see glossary](#)) valid in the Internet. Every computer or router participating in the Internet must have a uniquely assigned public IP address. This address is usually negotiated dynamically with the Internet Service Provider when a connection to the Internet is dialed. The Internet Service Provider assigns the negotiated IP address to the computer or router for the duration of an Internet session.

remote configuration

TR-069 ([see glossary](#))

splitter

DSL splitter ([see glossary](#))

Stick & Surf

Stick & Surf is a technique developed by AVM for the fast, simple, error-free and secure configuration of radio networks. This technique allows for the straightforward transmission of all important parameters of a radio network from the WLAN base station to any computer that is to be added to the radio network.

In this process the radio parameters used, including the WLAN channel, SSID and WLAN standard used, as well as security parameters like the encryption method and network key, are transferred almost fully automatically from the WLAN base station to the computer with the WLAN client that is to be connected.

subnet mask

The subnet mask indicates which part of an IP address ([see glossary](#)) is the network address and which the address of the computer. The network address defines what is called the subnet.

subnetwork

A local IP network can consist of one subnetwork or be divided into multiple subnetworks. The division into subnetworks is performed when the local IP network is configured. The subnetworks of a local IP network are also IP networks ([see glossary](#)).

switch

A switch is a device that connects multiple network devices with each other, for instance through an Ethernet.

In contrast to a hub, a switch can establish direct connections between the connected devices. This makes it possible to send data packets directly to specific recipients.

The entire data throughput is at the disposal of every connected device.

TCP/IP

short for Transmission Control Protocol / Internet Protocol

TCP/IP is the “language” of the Internet. TCP/IP is used to refer to a suite of protocols used for data communication over the Internet. TCP and IP are the network and transport protocols underlying most Internet services, including file transfer (FTP) and e-mail communication (SMTP). TCP/IP is available for practically all computer systems. TCP/IP thus offers the advantage of trouble-free communication between otherwise incompatible networks and systems.

TR-069

TR-069 is a technical directive that simplifies the automatic configuration of Internet access devices like the FRITZ!Box.

TR-069 describes the remote configuration of Internet access devices. In remote configuration the access and account data are automatically transmitted to the FRITZ!Box by the Internet provider. These may include the account data for the Internet connection, Internet telephone numbers and login data for Internet telephony, or both.

The Internet Service Provider saves the data to be transmitted on what is called an Auto Configuration Server (ACS). When the FRITZ!Box is connected with the broadband line (for instance, DSL), the data can be transferred automatically from the ACS to the FRITZ!Box. This relieves the user of the task of manually setting up the Internet and/or Internet telephone numbers in the FRITZ!Box.

Encryption and ID verification ensure that the automatic configuration of the FRITZ!Box can not be intercepted or performed by unauthorized parties.

Automatic configuration of the FRITZ!Box is possible only if the Internet Service Provider supports remote configuration with TR-069. Which data are transferred to the FRITZ!Box and how remote configuration is started depends on the provider. For some providers, for instance, the user must enter a start code in the FRITZ!Box user interface.

UMTS

short for Universal Mobile Telecommunications System

UMTS is a third-generation (3G) mobile radio standard with throughput rates of 384 Kbit/s to 7.2 Mbit/s.

The high throughput rates make it possible to support multimedia services. With special cards or USB sticks the Internet connection can also be provided for laptops or computers via UMTS.

update

A more recent version of software or firmware is called an update. Updates are often free of charge, resolve minor programming errors, and sometimes also offer new functions.

uplink port

The uplink port on a hub or switch is designed for connecting another hub or switch, or a router. In contrast to the uplink port, there is also a user port for connecting terminal devices. The send and receive directions are transposed on the uplink port. On some devices the port can change between normal and uplink mode by means of a switch.

upload

This term designates the procedure of transmitting files from one's own computer to another computer in the Internet.

UPnP

short for Universal Plug and Play (UPnP)

UPnP is an extension of the Microsoft Plug & Play standard that allows devices to network globally and to exchange services—without a central server or computer.

UPnP allows devices from all kinds of manufacturers (stereo systems, routers, printers, house controls) to be controlled via an IP-based network ([see glossary](#)), with or without central control through a gateway. It is based on a number of standardized network protocols and data formats. Expressed simplistically, devices can communicate with each other automatically using UPnP to exchange information.

Today the UPnP forum specifies the UPnP standard and certifies devices that are compliant with this standard.

UPnP AV

short for Universal Plug and Play Audio/Video

UPnP AV is a UPnP specification for the interaction between the media server, playback devices and devices controlling the streaming (transmitting a data stream) of audio, image and video data within networks. Media servers are devices that make audio, image and video data available upon request. Playback devices render the audio, image and video data (television, stereo systems, streaming clients). Control devices are remote controls (smartphone, remote control).

USB

short for Universal Serial Bus

The Universal Serial Bus is an interface for transferring data between a computer and connected devices. It was introduced in 1996. Today nearly all computers have multiple USB ports. USB is used, for instance, to connect many keyboards, mice, printers and external hard drives to the computer.

By now many other devices also have a USB port. For instance, many DVD and Blue-ray players can play back photographs, videos and music directly from a USB storage medium (hard drive, flash drive).

The Universal Serial Bus supports hot plugging. This means that USB devices can be connected without turning the computer off. The Universal Serial Bus also offers a 5-Volt power supply. This makes it possible to load devices at the USB port and operate USB devices that do not have a power supply of their own.

The Universal Serial Bus was introduced with the USB 1.0 specification in 1996. In 1998 came the reworked USB 1.1 specification, followed in 2000 by USB 2.0. With 480 Mbit/s, USB 2.0 provides for considerably higher throughput rates than USB 1.0/1.1 (12 Mbit/s).

VPN

short for Virtual Private Network

VPN serves to integrate devices from a neighboring network into your own network, without the networks having to be compatible with each other.

A VPN is generally an independent company network distributed over several locations, which uses the infrastructure of a public communications network to link its partial networks or to link individual computers to the rest of the network. A VPN uses tunneling technologies and typically builds on the infrastructure of the Internet.

Using a Virtual Private Network it is possible to use all network applications of the company network even from distant locations. This means it is possible to use the advantages of the network even over large geographical distances.

VPN facilitates optimum information flow without delay throughout the entire company, even to offices in other locations. E-mail servers, file sharing and other central applications of the company network can thus be made available via VPN even to distant branch offices, subsidiaries and home offices. With VPN, field representatives of a company can also be granted secure access to the company network.

VoIP

short for Voice over IP, also known as Internet telephony

Calls from the Internet are possible to and from the fixed-line network and mobile networks. Various Internet Service Providers and telephony carriers provide SIP-fixed-line gateways for this purpose. The gateways are used to produce voice connections between the Internet and conventional telephone networks.

In principle, VoIP calls can be made over any Internet connection. However, for convenient use with existing terminal devices, and for conversations with the fixed-line and mobile networks, it is important that the Internet Service Provider

support what is known as the SIP standard. SIP is the current standard defined for VoIP by the IETF (Internet Engineering Task Force).

WLAN

short for Wireless Local Area Network

The term WLAN designates the industry standard for wireless local networks passed by the Institute of Electrical and Electronics Engineers (IEEE) in 1997 under the title IEEE 802.11.

By means of WLAN technology, individual computers or network devices like printers or DSL access points can be linked wirelessly to an existing cable-connected local network (LAN), or LANs can be converted completely to a wireless structure. A further useful purpose for WLAN technology is to link segments of existing cable-connected networks.

Although WLAN was actually developed only for short-range connections, by cascading WLAN base stations or implementing transmission networks with high-power point-to-point radio transmission, even network segments located further away from each other can be linked or network participants in relatively remote locations can be economically and easily integrated into an existing network.

WLAN base stations often also serve as access points to the Internet in private or public institutions. Many airports, hotels and cafes, for instance, make WLAN hotspots available to their customers, either free or subject to a charge. Ultimately this has maneuvered WLAN into serious competition with mobile UMTS technology.

The application possibilities for wireless network communication also overlap with Bluetooth technology. For mobile devices with limited energy capacity Bluetooth is the more useful solution, however, as Bluetooth uses considerably less power than wireless LAN. What is more, Bluetooth technology is more flexible and thus can offer a greater bandwidth of potential applications.

Index

A

- access rights
 - user interface 26
- access rules 33
- accessories 102
- ambient conditions 97
- autochannel 54
 - see WLAN autochannel
- AVM Stick & Surf 19

B

- blocking Internet pages 33
- button
 - WLAN 10

C

- cable
 - network cable 97
- cable connection (broadband) ... 16, 30
- CE conformity declaration 108
- child protection 33
- connecting
 - computers 17
 - FRITZ!WLAN USB Stick 19
 - multiple computers 18
 - to electrical power 15
 - to network hub/switch 18
 - to LAN 17
 - to LAN port 17
 - to USB devices 71
 - WLAN 19
- copyright 107
- customer service 98

D

- declaration of CE conformity 108
- DHCP server
 - integrated 63
- disposal 109
 - electronic equipment 109
- DNSSEC 41
- documentation 98

- drilling template 110
- dynamic DNS 35

E

- ending operation 94
- energy consumption 97
- energy savings 79

F

- factory settings
 - DHCP server 63
 - IP address 63
 - radio network name 44
 - restoring with FRITZ!Box 94
- FAQs 99
- filter 33
- firmware 32
- FRITZ!WLAN Repeater N/G 47
- FRITZ!WLAN USB Stick 19

G

- guest access 44

H

- help
 - customer service 98
 - FAQs 99
 - manual 98
 - support team 99
 - user interface 98
 - videos 98
- home network 8, 60
 - see network
- HSPA 16, 30
 - see mobile telephone network
- HTTPS 36
- hub
 - network 18

I

imprint.....	107
information in the Internet	
FAQs	99
videos	98
instructions	
handling	14
security	13, 14
interfaces.....	9
Internet access	
regulating times	33
Internet connection	
configuration wizard.....	28
configure manually.....	28
configuring	28
over DSL	28
via cable modem	16, 30
via the mobile telephone	
network	16, 30
Internet filter.....	33
Internet Protocol Version 6.....	42
see IPv6	
Internet router.....	33
IP address	
changing	65
factory settings.....	63
in Linux	70
in Mac OS X.....	69
in Windows 7	66
in Windows Vista	67
in Windows XP	68
obtaining automatically.....	66
IP settings	62
IPv6	42

L

LAN connecting	17
LEDs.....	11
legal notice	107

M

manufacturer's warranty.....	100
media server	72
mobile telephone network	16, 30

N

network	8, 60
changing settings.....	65
connecting	17
factory settings.....	62
IP settings.....	62
network hub/switch	18
network overview	60
network settings.....	60
prioritization	36
UPnP settings	65
network cable	97
network devices	60
remote maintenance of computer.....	62
wake on LAN	62
night service	
for WLAN	45
notice	
legal.....	107

O

operation requirements	12, 12
------------------------------	--------

P

package contents	12
password protection	
user interface	26
physical specifications.....	97
PIN method	21
see WPS	
port forwarding.....	34
ports and interfaces	96
power consumption	97

R

radio network name	44
recovery	
electronic equipment.....	109
recycling	109
remote access.....	36, 39
see VPN	
repeater	
FRITZ!WLAN Repeater N/G	47

S

saving energy	79
security	
operating instructions	13, 13
user interface	26
WLAN	44
settings	
IP address	66
network	62
restoring	27
saving	27
software	
firmware	32
SSID	44
see radio network name	
starting operation	
requirements for operation	12
streaming	72
support	98
by E-mail	100
information in the Internet	98
switch	18
see network	
symbols	
in the manual	6

T

technical specifications	96
--------------------------------	----

U

UMTS	
Internet connection	16, 30
UPnP	
settings	65
USB	
accessing memory	72
connecting	9
devices	71
port	8
storage media	71
user interface	
opening	25
password protection	26
restoring settings	27
saving settings	27

V

videos	98
VPN	39
client	40
configuration wizard	40
remote access	39
supplementary software	40

W

wake on LAN	62
warranty	100
WDS	
WLAN range	48
Wi-Fi Protected Setup (WPS)	20
WLAN	19
base station	7, 9
frequency ranges	54
FRITZ!WLAN Repeater N/G	47
guest access	44
range	47
security	44
standards	49
switching on and off	10
Wireless Local Area Network	44
WPS	20
WLAN autochannel	54
WLAN button	10
WLAN connection	
FRITZ!WLAN USB Stick	19
with Stick & Surf	19
with WPS	20
WLAN devices	19
connecting by WPS	20
WLAN frequency ranges	54
WLAN security settings	
manual transfer	23
WPS	20
PIN method	21
push-button configuration	
(WPS-PBC)	20