ENGLISH

Introduction

Sandberg Wireless G54 Router allows you to share a broadband connection and local area network connection using both wireless and wired connections. The Sandberg Wireless G54 Router is easy to configure thanks to its user-friendly web interface. Its features include a range of security settings that you can configure to prevent uninvited guests. The router works with ADSL, xDSL, FWA and cable modem connections that support one of the four protocols Ethernet, PPPoE or PPTP or L2TP. Your Internet service provider can tell you whether your Internet connection is using one of these four standards. English manual.

System requirements

- Internet connection supporting Ethernet, PPPoE, PPTP or L2TP (with RJ45 connector).
- One or more computers with Ethernet adapter or Wireless Ethernet adapter

1 Installing the router

1.1 Role of the router on the network

A router acts as a connection point between two networks. A router is generally used to connect a local area network with multiple computers to the network of an Internet service provider. In other words, a router allows several computers to share an Internet connection. The Sandberg Wireless G54 Router is wireless, meaning that computers with wireless network cards can connect to it without the use of cables.

Figure 1 shows an example of a typical network setup, with two computers sharing an Internet connection.

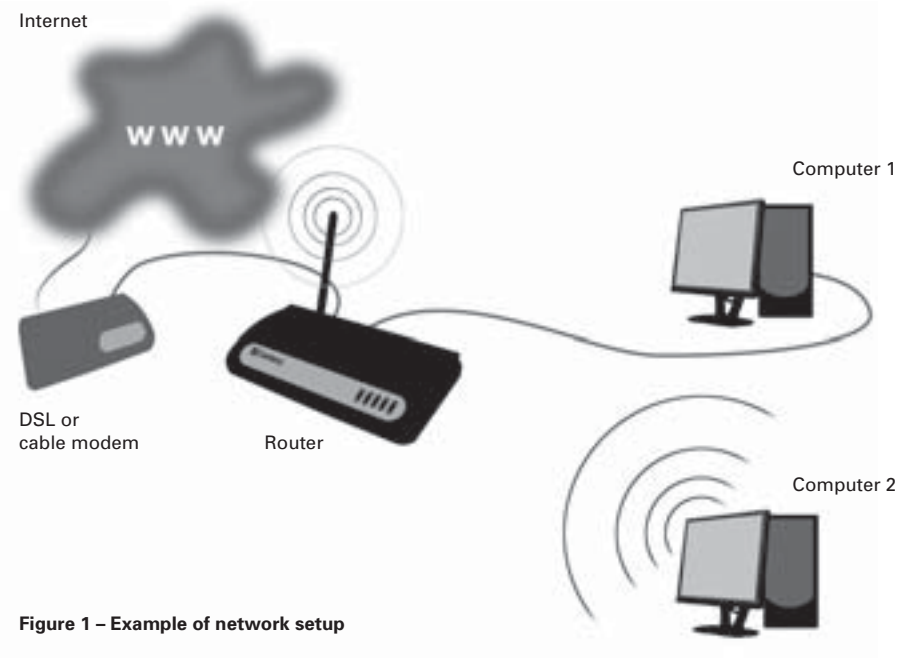

Figure 1 – Example of network setup

As the router's role is to create a bridge between two networks, it has one IP address for each network. One IP address represents the router on the Internet and is called the *external IP address*, and the other represents the router on the local area network and is called the *internal IP address*. Each of the computers on the local area network also has its own IP address. This can be allocated automatically by the router (using the router's DHCP function) or it can be specified manually on each computer.

Figure 2 shows a typical network setup, and the IP addresses that form part of that setup.

172.64.102.85 is the router's **external** IP address. When communicating with a computer over the Internet, it will be this address that the computer 'sees', regardless of which computer on the local area network is being used. The external IP address can either be **dynamic** or **fixed**, depending on the type of subscription set up with the Internet service provider. A dynamic IP address is one that is allocated by the Internet service provider, but it is not necessarily the same address all the time. A fixed IP address always remains the same.

192.168.2.1 is the router's **internal** IP address. This is the address of the router on the local area network, the one that all the computers on the network connect to in order to access the Internet.

192.168.2.100 is the IP address of a computer on the network. This can either be defined in Windows or be automatically allocated by the router.

192.168.2.101 is the IP address of a computer on the network. This can either be defined in Windows or be automatically allocated by the router.

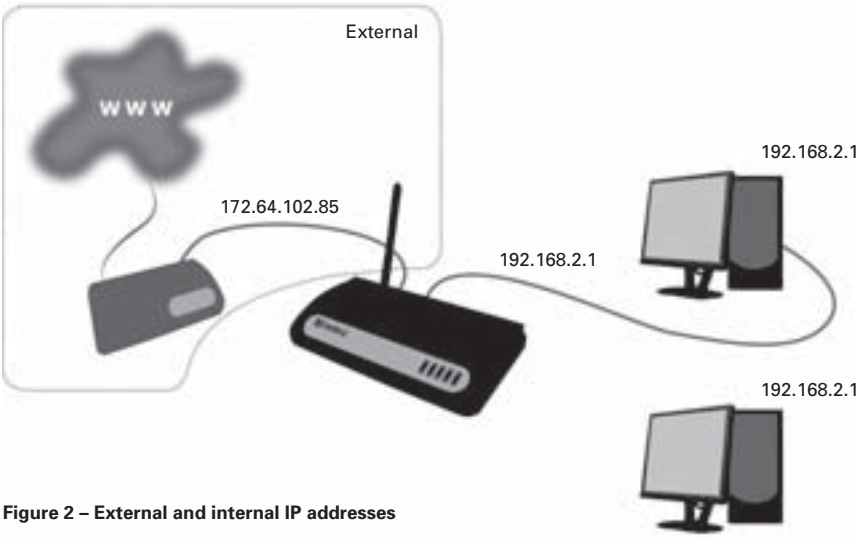

Figure 2 – External and internal IP addresses

1.2 Connecting the router

Figure 3 – Router ports

The router can function both as a router and an access point. The connection mode used with the router depends on how it is intended to function on the network.

- **Router** – Used if the Internet connection is to be shared between multiple computers, either wirelessly, with cables, or both.
- **Access Point** – Used if the Internet connection is already shared between multiple computers, e.g. via a router, and wireless access to the Internet is required. In this case, the role of the router is to provide wireless access to the existing router.

1. Connect the electrical plug to a mains socket and the small round connector on the power lead to the **12VDC** socket on the router. Check that the "Power" lamp lights up.
   - If you will be using the router function, connect the router's **WAN** port to your existing ADSL/ broadband connection using a network cable.
   - If you will be using the access point function, connect a network cable from the existing network (typically the existing router) to port 1, 2, 3 or 4 on the router.
2. Screw the antenna firmly into the thread on the far right. The antenna can be folded upwards to increase the signal strength.
3. Connect up to four computers to the ports marked 1 to 4 on the router. If you will only be connecting wirelessly, skip this step.
4. Start the connected computers.

Lamp indications

LED	Colour	Status	Status
PWR	Green	On	The router is on.
WLAN-G	Green	On Flashing Off	Wireless connection is active. Wireless connection transmitting data. Wireless connection is inactive.
WAN – 10/100M	Green	On Off	100 Mbit/s connection active. 10 Mbit/s connection active.
WAN – LNK/ACT	Green	On Flashing Off	WAN port connected. WAN port transmitting data. WAN port disconnected.
LAN – 10/100M	Green	On Off	100 Mbit/s connection active. 10 Mbit/s connection active.
LAN – LNK/ACT	Green	On Flashing Off	LAN port connected. LAN port transmitting data. LAN port disconnected.

Positioning and installation of the router

Drill template
To ensure the best possible wireless signal conditions, the router should be placed centrally in relation to the devices connecting wirelessly to it.

The package includes an installation kit containing four rubber feet, two screws and two rawlplugs. The rubber feet can be stuck to the base of the router to stand it on a flat surface.

If you wish to wall-mount the router, drill two holes in the wall 14 centimetres (5.51 inches) apart. At the back of this manual there is a drill template that you can cut out and use to ensure the holes are the correct distance apart. On the back of the router there are two sets of brackets, allowing it to be mounted with the connectors facing up or down.

2 Setting up the router

2.1 Configuring the computer's network settings

To access the router configuration, you need to set up the computers on the same network as the router. In other words, the computers must be set up to have their IP addresses automatically allocated by the router.
Do this as follows:

2.1.1 Windows® XP

1. Click **[Start]**, **[Control Panel]** and then **[Network and Internet Connections]**. Double-click **[Network Connections]**.
2. Double-click **[LAN Connection]**. Then click **[Properties]**.
3. Double-click **[Internet Protocol (TCP/IP)]** and select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
4. Click **[OK]** and close the **Local Area Connection Properties** dialog box by clicking **[OK]**.

The IP address will now be active.

2.1.2 Windows® 2000

1. Click **[Start]**, then **[Settings]** and **[Dial-up and Network Connections]**.
2. Double-click **[LAN Connection]**. Click **[Properties]**.
3. Double-click **[TCP/IP]** and select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
4. Click **[OK]** and close the **Local Area Connection Properties** dialog box by clicking **[OK]**.

The IP address will now be active.

2.1.3 Windows® 98SE/Me

1. Click **[Start]**, **[Settings]**, **[Control Panel]**. Double-click the **[Network]** icon.
2. Double-click **[TCP/IP]** and select **Obtain an IP address automatically**.
3. Click **[OK]** and close the **Network** dialog box by clicking **[OK]**.

Restart the computer.

The IP address will now be active.

2.2 Configuring the router

NB:
If you will be using the router as an access point only, the following steps can be skipped. However, the router's wireless security function should be enabled. (See section 2.3)

If you will be using the router wirelessly, the computer must be connected to the router's wireless network before the following steps can be carried out. See the documentation that came with the computer's wireless network card for information on how to connect to a wireless network.

1. Start your Internet browser (e.g. Internet Explorer®).
2. Type **http://192.168.2.1** in the browser's address bar and press **Enter**.
3. In the **Username** field, type **admin**.
4. In the **Password** field, type **1234**. Click **[OK]**.
5. Click the **[Quick Setup]** button.

Figure 4 – Router configuration utility

The default router configuration wizard will now start.

Time Zone

1. Select the appropriate time zone.
2. The **Time Server Address** field allows you to enter the IP address of a time server to set the router clock automatically. The field contains a default value, but can be changed if you wish to use a different time server.
3. The **Daylight Savings** field indicates whether the router will switch automatically between summer time and winter time. Check the box **Enable Function**, and enter the dates for changing to summer time or winter time.
4. Click **[Next]**.

Broadband Type
Here you can enter the type of connection used by the router. Contact your Internet service provider if you are unsure which type of Internet connection you have.

- Select ***Cable modem*** if you have a cable modem or other type of Internet connection without a fixed IP address.

  - **Host name**: Can be set to any name unless specified by your Internet service provider. The MAC address is automatically set to the MAC address of your cable modem. This should not be changed unless specified by your Internet service provider.
  - **Clone MAC address**: This function is usually not required for default setup. This button can be used to specify the MAC address of the computer's network card as the actual MAC address of the router.
  - When your changes are complete, click **[OK]**. The router will then confirm the changes. Click **[OK]**.
  - Close the window by clicking the cross in the top right corner.

- Select ***Fixed-IP xDSL*** if you have an xDSL or Ethernet connection with a fixed IP address.

  - **IP address assigned by your service provider**: Enter the IP address assigned by your Internet service provider.
  - **Subnet mask**: Enter the subnet mask assigned by your Internet service provider.
  - **DNS address**: Enter the DNS addresses assigned by your Internet service provider.
  - **Service provider gateway address**: Enter the gateway address assigned by your Internet service provider.
  - When your changes are complete, click **[OK]**. The router will then confirm the changes. Click **[OK]**.
  - Close the window by clicking the cross in the top right corner.

- Select ***Dial-up xDSL (PPPoE)*** if you have an xDSL/FWA connection that uses PPPoE.

  - **User name**: Enter the username assigned by your Internet service provider.
  - **Password**: Enter the password assigned by your Internet service provider.
  - **Service name**: Enter the service name assigned by your Internet service provider. If you have not been assigned a service name by your Internet service provider, this field can be left blank.
  - **MTU** (1400-1492): The router will propose 1492. You can accept this unless your Internet service provider recommends a different value.
  - **Connection type**: There are three options to choose from:
    Continuous – the router maintains a permanent connection to your Internet service provider.
    Connect on demand – the router only connects when necessary and disconnects itself after a set period of time (see **Idle time**).
    Manual – you activate the connection through the router yourself when you need it.
  - **Idle time**: Specifies the period of time after which the router will disconnect when it is not in use. This function is only used if the **Connection type** is set to **Connect on demand**.
  - When your changes are complete, click **[OK]**. The router will then confirm the changes. Click **[OK]**.
  - Close the window by clicking the cross in the top right corner.

- Select ***PPTP*** if you have a connection of this type.
  [**NB**: This connection is rarely used in Scandinavia.]

  - **WAN Interface Settings**: Set the router to obtain an IP address automatically, or enter the IP address, subnet mask and gateway if these have been assigned to you by your Internet service provider.
  - **PPTP Settings**: Enter the information assigned by your Internet service provider in the appropriate fields.
  - When your changes are complete, click **[OK]**. The router will then confirm the changes. Click **[OK]**.
  - Close the window by clicking the cross in the top right corner.

The default router configuration is now complete. However, before using the router, you should secure it against unauthorised wireless access. The following section contains information on how to do this.

2.3 Securing a wireless network

If you are using the router's wireless functionality, the network must be secured against unauthorised access by enabling one of the router's built-in security features. This protects authorised network users against unauthorised access from the outside.
The router can use one of the following security features:

- **WEP**
- **WPA pre-shared key**
- **WPA RADIUS**

All computers that connect wirelessly to the router must use the same type of security as the router. It is therefore important to select a security method supported by all the network cards on the network. For more information on this, see the user guide for the individual network cards on the network.

For additional security, the **MAC Address Filtering** function can be used. See section 2.3.4 for information on this.

Configuration of the various security features is described in the following sections.

2.3.1 Configuring WEP

1. Click **[General Setup]**.
2. Click **[Wireless]**, then **[Security Settings]**.
3. Under **Encryption**, select ***WEP***.
4. Under **Key Length**, select the encryption strength. You can select either ***64-bit*** or ***128-bit***. For greatest security, ***128-bit*** is recommended.
5. Under **Key Format**, select the format for entering security codes. You can select either **HEX** (digits and/or letters from A to F) or **ASCII** (letters and/or digits).
6. Under **Default TX Key**, select the security code to use as default.
7. In the fields **Encryption Key 1-4**, enter up to four security codes. If you enter multiple codes, computers can access the network wirelessly by entering any one of them. The codes must comply with the format given in **Key Length** and **Key Format**. Both upper and lower case letters can be used.
   64-bit HEX – 10 digits and/or letters from A to F
   128-bit HEX – 26 digits and/or letters from A to F
   64-bit ASCII – 5 letters and/or digits
   128-bit ASCII – 13 letters and/or digits
8. Click **[Apply]**.
9. Click **[Continue]** to change more settings or **[Apply]** to restart the router for the new settings to take effect.

2.3.2 Configuring WPA pre-shared key

1. Click **[General Setup]**.
2. Click **[Wireless]**, then **[Security Settings]**.
3. Under **Encryption**, select ***WPA pre-shared key***.
4. Under **WPA Unicast Cipher Suite**, select the type of encryption to use. You can select **WPA(TKIP)**, **WPA2(AES)** or **WPA2 Mixed**. Note that all devices connecting to the network must support the encryption type.
5. Click **[Apply]**.
6. Click **[Continue]** to change more settings or **[Apply]** to restart the router for the new settings to take effect.

2.3.3 WPA RADIUS

This type of security is for advanced users and requires a separate RADIUS server. WPA RADIUS is typically used in larger corporate networks, and is not recommended for private use. Documentation on configuring the router for WPA RADIUS can be found in the English manual on the CD provided.

2.3.4 Configuring MAC Address Filtering

All network devices have a unique code called the **MAC address**.
Mac Address Filtering is an extra security feature that ensures that only network devices with MAC addresses approved by the router can connect to the wireless network.

1. Click **[General Setup]**.
2. Click **[Wireless]**, then **[Access Control]**.
3. In the **MAC address** field, enter a MAC address.
4. If necessary, enter a comment for the MAC address in the **Comment** field.
5. Click **[Add]** to add the MAC address to the list of approved addresses.

How to discover the MAC address of a wireless network card

Windows® XP
1. Click **Start**, then **Control Panel**, then **Network and Internet Connections**, then **Network Connections**.
2. Double-click the icon for the wireless network connection, click the **Support** tab and then click **Details**...
3. The value indicated for **Physical address** is the network card's MAC address.

Windows® 2000
1. Click **Start**, then **Run**. Type "**cmd**" in the field and press **Enter**.
2. Type "**ipconfig/all**".
3. Locate the line with "**Description**..." followed by the name of the wireless network card. The value indicated for **Physical address** is the network card's MAC address.

Windows® 98SE / ME
1. Click Start, then **Run**. Type "**winipcfg**" in the field and press **Enter**.
2. Click the little arrow and select the wireless network card from the menu.
3. The value indicated for **Network card address** is the network card's MAC address.

3 Advanced setup

Advanced setup enables you to define specific settings for your network's security policy, data traffic, etc. This requires specialised knowledge, including network technologies and security policies, and is only recommended for users with experience in these areas. These settings are not usually required for standard setup.

1. Start your Internet browser (e.g. Internet Explorer®).
2. Enter "**http://192.168.2.1**" in the browser's address bar and press **Enter**.
3. In the **Username** field, type "**admin**".
4. In the **Password** field, type "**1234**".
5. If you want this to be remembered next time you log on, check the box **Remember password**. Click [**OK**].
6. Click the [**General Setup**] button.

3.1 System

The System menu contains settings for the time zone, password and remote access to the router.

3.1.1 Time Zone

- Select the time zone in the **Set Time Zone** menu.
- Enter the IP address of a time server in the **Time Server Address** field. The field contains a default value, but can be changed if you wish to use a different time server.
- Check the box next to **Enable Function** and set the start and end date for summer time in the **Daylight Savings** field.
- Click [**Apply**] to confirm the settings.

3.1.2 Password Settings

To change the password for access to the router, follow the steps below.

- Enter the current password in the **Current Password** field.
- Enter a new password in the **New Password** and **Confirmed Password** fields.
- Click [**Apply**] to confirm the settings.

3.1.3 Remote Management

Settings for remote access to the router configuration utility. Remote access allows the router to be configured from a computer via the Internet.
NB: If you enable remote access, it is essential that you change the default password for router access to a password of your choosing. See section 3.1.2.

- Check the box next to **Enabled** to enable remote access.
- In the **Host Address** field, enter the IP address of the computer on the Internet that will have remote access to the router configuration utility.
- Enter IP address **0.0.0.0** to give all computers remote access.
- Click [**Apply**] to confirm the settings.

3.2 WAN

Settings for manual configuration of the connection type. The settings are the same as those configured in **Quick Setup**. See section 2.2 (subsection ***WAN Type***) for information on the various settings.

3.3 LAN

For setting the router's IP address and configuring its DHCP server.

3.3.1 LAN IP

- Enter the desired IP address for the router in the **IP Address** field.
- Enter the subnet mask in the **IP Subnet Mask** field.
- Click [**Apply**] to confirm the settings.

3.3.2 DHCP Server

- In the **Start IP** field, enter the first IP address in the range that the DHCP server can allocate.
- In the **End IP** field, enter the last IP address in the range that the DHCP server can allocate.
- If necessary, the router's DHCP server can be disabled by selecting **Disabled** in the ***DHCP Server*** field.
- Click [**Apply**] to confirm the settings.

3.4 Wireless

Enable or disable wireless access to the router. By default, this function is enabled.

- Select **Enable** to enable wireless access to the router, or **Disable** to disable the function.
- Click [**Apply**] to confirm.

3.4.1 Basic Settings

- In the **ESSID** field, enter the name for the wireless network. This is the name that will be shown when Windows® displays a list of available wireless networks.
- **AP, Band** and **Channel Number** are advanced settings and should only be changed in special circumstances.
- Click [**Show Active Clients**] to view a list of wireless devices currently connected to the router.

3.4.2 Advanced Settings

This menu contains advanced settings for the wireless network. They require thorough knowledge of wireless networking technology and do not normally need to be changed. Documentation on these functions can be found in the English manual on the CD provided.

3.4.3 Security Settings

See section 2.3.

3.4.4 Access Control

See section 2.3.4.

3.5 QoS

- Reserve bandwidth for specific web applications.
- Limit bandwidth usage for specific web applications.

Quality of Service (QoS) is a function that allows the router to prioritise bandwidth usage so that specific services are always guaranteed a certain level. This can be very useful for services such as IP telephony, to ensure that call quality is not diminished when there is heavy network traffic. QoS can also be used to impose a maximum limit on the bandwidth usage of certain applications.

To use Quality of Service, one or more rules must be set up to define the bandwidth requirements for certain applications.

The router has no direct link to applications on the computer, so the only way to control the applications' network traffic is to configure rules regulating traffic on the network ports used by the applications. You therefore need to know which network ports are used by an application before you can set up a Quality of Service rule. The ports an application uses can normally be found in the application's written documentation or on its website.

3.5.1 QoS menu

The QoS menu contains a list of rules that have been set up. Every rule on the list has a priority (**Priority**). The rule with the highest priority is allocated bandwidth first, and so on down the list. Network traffic that is not covered by user-defined rules is allocated bandwidth last of all.
NB: If the total bandwidth allocated to user-defined rules exceeds the bandwidth the Internet connection can deliver, no bandwidth will be available for other applications.

- **Enable QoS** – Enable Quality of Service. Check this box if you wish to use Quality of Service. Click [**Apply**] to confirm.

3.5.2 Adding a QoS rule

1. Click [**Add**].
2. Enter a name for the rule in the **Rule Name** field. This could be the name of the application the rule relates to.
3. Under **Bandwidth**, the first field allows you to select whether the rule will apply to incoming traffic (**Download**) or outgoing traffic (**Upload**). If you need to establish rules for both incoming and outgoing traffic, you must set up one rule for each.
4. In the second field, enter the amount of bandwidth you wish to reserve. This must be given in kilobits per second (kbps).
5. In the third field, indicate whether the bandwidth entered is a guaranteed minimum (**Guarantee**) or a maximum limit that cannot be exceeded (**Max**).
6. In the **Local IP Address** field, enter the local IP addresses the rule will apply to. Enter a start address and end address in the fields. For example, ***192.168.2.1-192.168.2.255*** would represent all the computers on the network 192.168.2.xxx (where "xxx" is a number between 1 and 255)
7. In the **Local Port Range** field, enter the local network ports the rule should apply to. If the application only uses a single port, enter it in this field. Otherwise a range of ports can be specified by using a hyphen. For example: ***800-1000***, which specifies all ports between 800 and 1000.
8. In the **Remote IP Address** field, enter an IP address on the Internet, from which all traffic will be subject to the rule. Traffic not originating from this address will not be affected. It is not normally necessary to enter a value for this field.
9. In the **Remote Port Range** field, enter one or more ports, from which all traffic will be subject to the rule. Traffic not originating from these ports and the address entered under **Remote IP Address** will not be affected. It is not normally necessary to enter a value for this field.
10. **Traffic Type** – Choose between a range of predefined types of network traffic. If you select a type here, you do not need to enter a value for **Local Port Range**. The options are:
    a. **None** – No traffic type is selected. Select this if a value has been entered for **Local Port Range**.
    b. **SMTP** – Outgoing email.
    c. **HTTP** – World Wide Web.
    d. **POP3** – Incoming email.
    e. **FTP** – FTP server.
11. **Protocol** – Select the network protocol the rule applies to. You can select either **TCP** or **UDP**. Information on the protocols used by an application can be found in the application's documentation. If an application uses both protocol types, two QoS rules must be set up.
12. Click [**Save**] to add the rule. Click [**OK**]. Click [**Apply**].

3.5.3 Moving a QoS rule

If a rule needs to be allocated higher or lower priority, it can be moved up or down the list.
1. To select a rule, check the box next to it in the **Select** column.
2. Click [**Move Up**] to give the rule higher priority or [**Move Down**] to give it lower priority.
3. Click [**Apply**].

3.5.4 Deleting a QoS rule

1. To select a rule, check the box next to it in the **Select** column.
2. Click [**Delete Selected**].
3. Click [**OK**] in the two boxes that appear.
4. Click [**Apply**].

3.5.5 Deleting all QoS rules

1. To select a rule, check the box next to it in the **Select** column.
2. Click [**Delete All**].
3. Click [**OK**] in the two boxes that appear.
4. Click [**Apply**].

3.6 NAT

NAT (**Network Address Translation**) is a technology that allows multiple computers on a local area network to share the same external IP address. The way this works is that the router manages all the network traffic originating from the computers on the network and sorts incoming network traffic so it is redirected to the right computer. However, this may cause a problem for network traffic that is not initiated at the request of a computer on the local area network.

A typical scenario is when a computer on the local area network is set up as a server. In this case, a computer on the Internet would connect to the router's external IP address. However, this network request does not indicate which computer on the local area network it is addressed to, and the router therefore has no means of knowing where to forward it. This is solved by setting up the router's NAT function so that it forwards incoming network traffic on certain network ports to a specific IP address on the local area network.

Example: An FTP server is set up on a computer on the network with the IP address 192.168.2.100. FTP uses network port 21 by default. The router's NAT function is set up to forward all incoming traffic on port 21 to IP address 192.168.2.100.

It may also be necessary to configure NAT for applications such as IP telephony, file sharing and online gaming to work properly.

NAT can be configured in two modes: ***Port Forwarding*** and/or ***Virtual Server***. These are described in the following sections.

3.6.1 Port Forwarding

Port Forwarding means setting up rules specifying the type of network traffic to be redirected to a particular computer on the local area network.

NB: For Port Forwarding to work as intended, the computer that network traffic is forwarded to must be configured with a static IP address. See section **3.6.3** for information on this.

1. Click [**General Setup**]. Click [**NAT**]. Click [**Port Forwarding**].
2. Check the box next to **Enable Port Forwarding**.
3. Enter the IP address of the computer on the local area network to redirect to in the **Private IP** field.
4. Specify the type of network traffic to redirect under **Type**. Select **TCP**, **UDP** or both (**Both**). The network traffic type depends on the type of application used on the computer that traffic is forwarded to. If necessary, see the application's documentation for details on this.
5. Enter the ports from which network traffic should be forwarded in the **Port Range** field.
6. If you wish, enter a comment in the **Comment** field.
7. Click [**Apply**].

You can edit the defined rules in the list at the bottom of the screen.
Delete a rule – Check the box next to the rule in the **Select** column. Click [**Delete Selected**].
Delete all rules – Click [**Delete All**].

3.6.2 Virtual Server

Virtual Server works in almost the same way as Port Forwarding. The only difference is that network traffic arriving at an external network port can be forwarded to another network port on a computer on the local area network. This might be useful if you have a server set up on the local area network that does not use the default port.

Example: An FTP server is set up on a computer on the local area network with the IP address 192.168.2.100. This server does not use default port 21, but instead uses port 3015.
Virtual Server can be set up to forward all incoming traffic on port 21 to IP address 192.168.2.100 on port 3015. This means that users of the FTP server do not have to change the port number used by their FTP application to connect to the server.

NB: For Virtual Server to work as intended, the computer that network traffic is forwarded to must be configured with a static IP address. See section **3.6.3** for information on this.

1. Click [**General Setup**]. Click [**NAT**]. Click [**Virtual Server**].
2. Check the box next to **Enable Virtual Server**.
3. Enter the IP address of the computer on the local area network to redirect to in the **Private IP** field.
4. Enter the port on the local area network to redirect traffic to in the **Private Port** field.
5. Specify the type of network traffic to redirect under **Type**. Select **TCP**, **UDP** or both (**Both**). The network traffic type depends on the type of application used on the computer that traffic is forwarded to. If necessary, see the application's documentation for details on this.
6. Enter the external ports from which network traffic should be forwarded in the **Public Port** field.
7. If you wish, enter a comment in the **Comment** field.
8. Click [**Apply**].

You can edit the defined rules in the list at the bottom of the screen.
Delete a rule – Check the box next to the rule in the [**Select**] column. Click [**Delete Selected**].
Delete all rules – Click [**Delete All**].

3.6.3 Specifying a static IP address in Windows®

In certain circumstances it may be useful to ensure that one or more computers on the local area network always have the same IP address. This is particularly relevant when setting up NAT. (See section 3.6.) This section describes how to configure a static IP address.

Specifying a static IP address in Windows® XP
1. Click [**Start**]. Click [**Control Panel**].
2. Click [**Network and Internet Connections**], then [**Network Connections**].
3. Double-click [**LAN Connection**]. Click [**Properties**].
4. Double-click [**Internet Protocol** (**TCP/IP**)].
5. Check **Use the following IP address** and enter the desired IP address in the **IP address** field.
6. Click in the **Subnet mask** field. The mask 255.255.255.0 is entered automatically. Click [**OK**].
7. Click [**OK**] to close the window. Click [**Close**] in the last window.

Specifying a static IP address in Windows® 2000
1. Click [**Start**], then [**Settings**] and [**Dial-up and Network Connections**].
2. Double-click [**LAN Connection**]. Double-click [**Internet Protocol** (**TCP/IP**)].
3. Check **Use the following IP address** and enter the desired IP address in the **IP address field**.
4. Click in the **Subnet mask** field. The mask 255.255.255.0 is entered automatically.
5. Click [**OK**] and close the **Local Area Connection Properties** dialog box by clicking [**OK**].

Specifying a static IP address in Windows® 98SE/ME

1. Right-click [**Other Computers**] on the desktop. Click [**Properties**].
2. Double-click [**LAN Connection**]. Click [**Properties**].
3. Find the protocol for the computer's network card that begins with "**TCP/IP ->**". Double-click it.
4. Select the **IP address** tab. Check **Enter an IP address** and enter the desired address in the **IP address** field.
5. Enter the mask 255.255.255.0 in the **Subnet mask** field. Click [**OK**].
6. Click [**OK**] in the last window.
7. Restart your computer.

3.7 Firewall

The router's built-in firewall can be configured to protect against commonly occurring hacker attacks. It is also possible to block or authorise specific MAC addresses and/or IP addresses, and to block access to certain websites on the Internet.

- Select **Enable** to enable the firewall on the router, or **Disable** to disable the function.
- Click [**Apply**] to confirm.

3.7.1 Access Control

Configuration of the MAC addresses that can access the router. This works in the same way as **Access Control** described in section 2.3.4, but here it also applies to the cabled network as well as traffic from the Internet.

- Check the box next to **Enable MAC Filtering** to enable the function.
- In the **Client PC MAC address** field, enter a MAC address.
- If necessary, enter a comment for the MAC address in the **Comment** field.
- Select **Deny** (to block the address) or **Allow** (to allow the address).
- Click [**Add**] to add the address to the list.
- Click [**Apply**] to confirm.

3.7.2 URL Blocking

Block particular addresses on the Internet to prevent them from being accessed by computers on the local area network.

- Check the box next to **Enable URL Blocking** to enable the function.
- Enter an Internet address in the field **URL / Keyword** and click [**Add**] to add it to the list.

3.7.3 DoS (Denial of Service)

Block commonly occurring hacker attacks.

- Select the types of hacker attack to block by selecting them on the list.
- Click [**Apply**] to confirm.

3.7.4 DMZ

If a computer on the local area network is running an application that is incompatible with NAT and firewalls, the computer can be configured to bypass these functions in its communication.

- Check the box next to **Enable DMZ** to enable the function.
- Specify whether your Internet connection has a dynamic or static IP address in the **Public IP Address** field. If the IP address is static, specify the address in the **Static IP** field.
- Specify the IP address of the computer on the local area network whose communication will bypass NAT and firewall in the **Client IP Address** field.
- Click [**Apply**] to confirm.

Troubleshooting

I cannot connect to the router when I type *http://192.168.2.1* **in my browser.**
- Check that the originating computer is connected to the router's wireless network. See section 2.2.
- Check that the originating computer is configured to be automatically allocated an IP address. See section 2.1.
- If necessary, try connecting the computer directly to port 1 on the router using a network cable.

The router cannot be detected by any wireless devices in the vicinity.
- Check that the "WLAN" LED on the router is on.
- Check that the router is within range of the wireless devices. Try repositioning the router or the wireless device trying to connect to it. The number of walls and ceilings, their thickness and materials, are all factors that affect the strength of the wireless signal.
- Check that the wireless devices are connected to the correct wireless network. See the documentation for the wireless devices for information on this.

Unable to connect to the router from a wireless device.
- Check that the security settings are appropriate for the wireless devices trying to connect to the router. See section 2.3 and the documentation for the wireless device for information on security settings.

The Internet connection is unstable when using PPPoE.
- Try changing the MTU value to 1440 (see section 2.2), or contact your Internet service provider for further information.

If you need further help or assistance in connection with your Sandberg product, you can see details about this on the penultimate page of these instructions.

Enjoy your Sandberg Wireless G54 Router.