

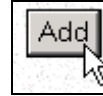
3. Click on the **Add** button to expand your WDS.

On the **Add WDS Link** screen that shows:

2. Fill up the **Partner Address** field with the MAC address of the device to include in your WDS, using the format xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or a mix of : and -, and where x can take any hexadecimal value 0-9 or a-f.
3. Use the **Status** option to control whether you want to **Enable** this particular WDS link or to **Disable** it.

To illustrate, we chose to add a WDS link with partner address **56:aa-0d:e4-f5-12** and to enable it.

4. Click on the **Apply** button.



Add WDS Link

Partner Address

Status

WDS Status

WDS link	Partner Address	Status
1	56-aa-0d-e4-f5-12	Enable

WDS link	Partner Address	Status
1	56-aa-0d-e4-f5-12	Enable

Edit WDS Link

Partner Address

Status

4. The **WDS Status** page will be updated as shown above left.

If you want to modify the status entry for a WDS link:

1. Select the radio button on the left of that particular link as illustrated below left.
2. Click on the **Edit** button.

The 3^d screen left will show.

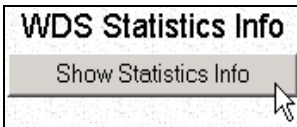
3. Click on the **Apply** button for the change you made to take effect.

5

If you want to delete a WDS link:

1. Select the radio button on the left of that particular link as illustrated on the right.
2. Click on the **Remove** button.

An updated **WDS Status** page will be displayed.



WDS Statistics						
WDS Link	rxTotal	rxUni	rxMulti	txTotal	txUni	txMulti
1	0	0	0	35	9	26

Refresh Back

WDS link	Partner Address	Status
☒ 1	56-aa-0d-e4-f5-12	Enable



WDS Status		
WDS link	Partner Address	Status

6

To view **WDS Statistics Info**:

Click on the **Show Statistics Info** button.

The **WDS Statistics** table shown on the left will be displayed.

Click on the **Refresh** button to refresh the page.

Alternatively:

Click on the **Back** button to return to **WDS Status** page.



NOTE:

- If the WDS-enabled access points are required to support too many operational wireless clients, you may find end-to-end throughput to be low (depending on the applications).
- End-to-end latency may become an issue in a long WDS chain configuration.
- In the **WDS Setup**:
 - o If **WDS Global Control** is Disabled, every WDS link will be closed regardless of its status.
 - o When **WDS Global Control** is set to Enabled, the status of every WDS link that you want to include still needs to be individually Enabled.

**NOTE:**

- Although they may belong to different SSIDs, all the WDS links have to be configured in the same channel and use the same encryption key, if the encryption feature is enabled, to be able to communicate with one another.
- In the **WDS Statistics** table:
Each entry corresponds to a particular WDS link and for each link, the parameters listed are:
 - o *WDS Link*: identifier assigned to the link
 - o *rxTotal*: total number of packets received (inclusive of *rxUni* & *rxMulti*)
 - o *rxUni*: number of unicast packets received
 - o *rxMulti*: number of multicast or broadcast

Parallel Broadband **exclusive!**

The NetPassage WPE54G is equipped with Compex's exclusive **Parallel Broadband** technology which not only implies scalable Internet bandwidth but also highlights Load Balancing and Fail-Over Redundancy features.

Load balancing

A network built around multiple WPE54G's arranged in cascade and running under Parallel Broadband enables you to maintain a balance on the Internet traffic generated by your private network over multiple broadband connections, thus achieving the effect of aggregated bandwidth!

Fail-Over Redundancy

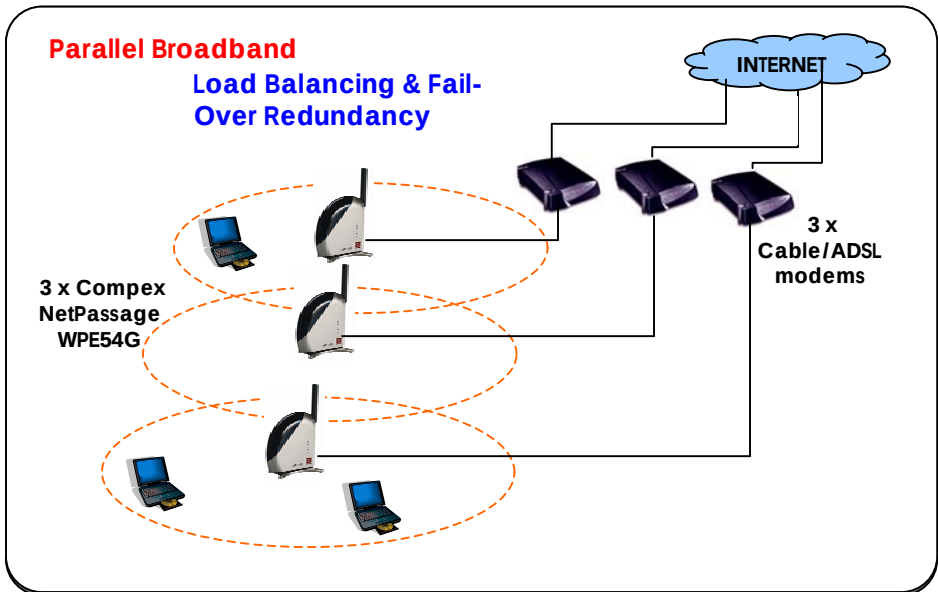
In case one of your broadband connections should fail, the WPE54G in cascade will automatically switch over to the operational broadband channels so that your network is not disrupted.

Ease of implementation

The Parallel Broadband implementation allows each WPE54G unit in the network to connect to its individual broadband Internet service account. There is no restriction to

the type of broadband Internet account that a WPE54G can connect to (whether Cable or ADSL). Indeed, your network may run with one WPE54G on Cable Internet, while the other WPE54Gs connect to ADSL.

The diagram below illustrates an application of Parallel Broadband in a network.



To learn more about Parallel Broadband, please read the whitepaper at www.cpx.com or www.compex.com.sg.

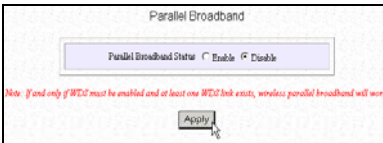
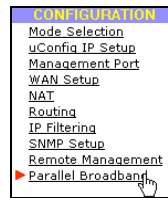
The next steps will show you how to enable Parallel Broadband in your network:

To begin with, for every WPE54G in your network, ensure that:

- It is properly configured to connect to its specific broadband Internet account.
- It is connected to an unused Ethernet port in the network.
- It is running Compex's Wireless Distribution System (WDS) feature, which can be enabled via the web-based configuration as illustrated in the previous section.
- It is correctly configured with the Parallel Broadband option as shown below.

Parallel Broadband

- 1 Click on **Parallel Broadband** from the **Configuration** menu.



- 2 The Parallel Broadband feature is *Disabled* by default.

1. Select to **Enable** the **Parallel Broadband Status** radio button.
2. Click on the **Apply** button for your selection to take effect.
3. Repeat this for the other WPE54Gs in your network to enable them to communicate with each other and assign new users to the gateway with the smallest load, so that there is approximately the same number of users on each gateway.



NOTE: The **Parallel Broadband** function for broadband Internet sharing can only be implemented if:

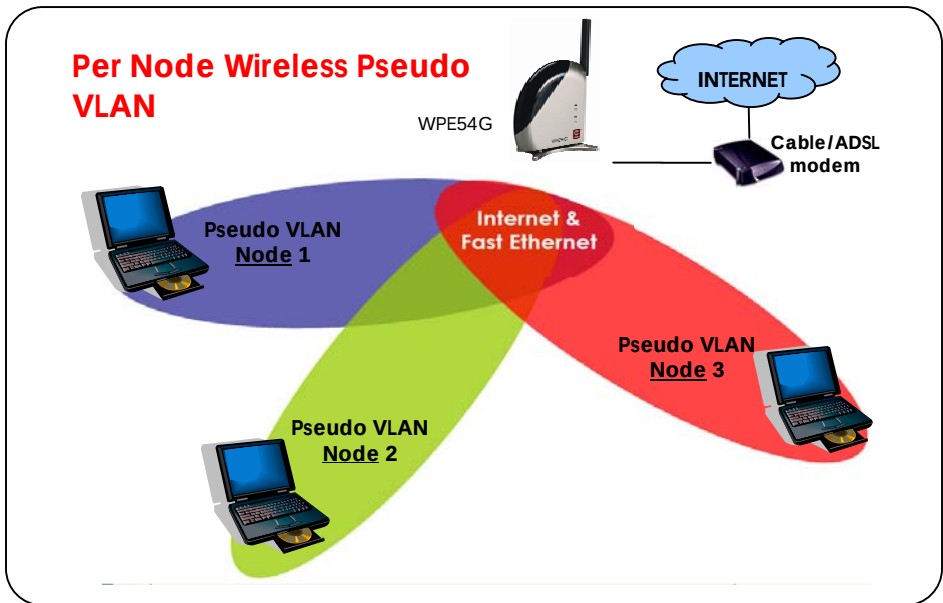
- There is more than one WPE54G unit in your network
- Each WPE54G unit in the network is running the Wireless Distributed System (WDS) feature.

Wireless Setup – The Wireless Pseudo VLAN

Wireless Pseudo VLAN featured on the WPE54G acts by segregating a single wireless LAN into multiple virtual LANs so that communication is possible only among wireless clients within the same VLAN. The WPE54G enables you to create virtual LANs containing either a single user, and referred to as *Wireless Pseudo VLAN Per Node*, or a group of users, termed as *Wireless Pseudo VLAN Per Group*

Wireless Pseudo VLAN Per Node

When implemented, this mode isolates each wireless client into its own pseudo VLAN. Wireless clients can therefore access resources on the wired network but are unable to see each other or access each other's data. This is illustrated in the following diagram.



The following steps demonstrate how to set up the *Wireless Pseudo VLAN per Node* mode.

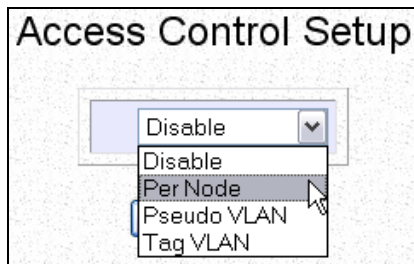
Wireless Pseudo VLAN

Per Node:

expert

- 1 Click on the **Access Control** button.

The Access Control Setup menu shown on the right will appear.



2

The Wireless Pseudo VLAN function is *Disabled* by default.

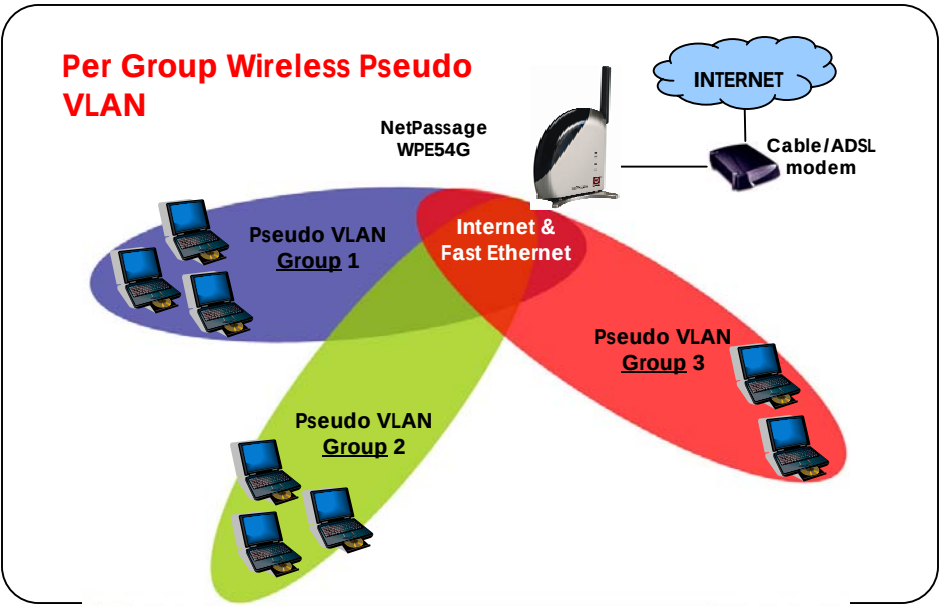
1. Select **Per Node** from the drop-down list.
2. Click on the **Apply** button.

Access control changed to PerNode will appear in the Message Window.

Wireless Pseudo VLAN Per Group

The WPE54G can configure up to four ‘groups’ of wireless clients identified by their MAC address. Whenever a wireless client requests network access, the WPE54G will first verify whether its MAC address is present in any of the Pseudo VLAN groups. If it is, the WPE54G will grant the client access to all the wired system resources and to all other wireless clients belonging to the same Pseudo VLAN group only.

The diagram depicts an example of a pseudo VLAN per group.



The following steps demonstrate how to set up the *Wireless Pseudo VLAN per Group* mode.

Wireless Pseudo VLAN

Per Group:

expert

- 1 Click on the **Access Control** button.

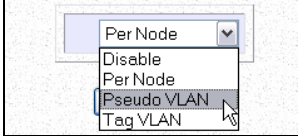
The Access Control Setup menu shown on the right will appear.

Access Control Setup

Disable ▼

Apply Help

Access Control Setup

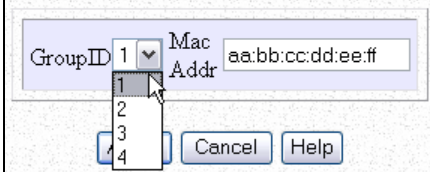


3

The **MAC Address List** enables you to manage specific VLAN groups by adding or deleting clients through their MAC address.

Click on the **Add** button.

Add MAC address



2

The Wireless Pseudo VLAN function is *Disabled* by default.

1. Select **Pseudo VLAN** from the drop-down list.
2. Click on the **Apply** button.

Access control changed to **PerGroup** will appear in the Message Window and the page shown in Step 3 will appear.

Access Control



Note: Changes made will only take effect after rebooting.

Apply Help

4

1. Select a group number from the **Group ID** drop-down list.

We illustrate with Group ID **1**.

2. Fill in the **Mac Addr** field with the MAC address of the client in the format **xx:xx:xx:xx:xx** or **xx-xx-xx-xx-xx-xx**, where x is any value within the range 0-9 or a-f.

We illustrate with **aa:bb:cc:dd:ee:ff**.

3. Click on the **Apply** button.

5

The updated **Mac Address List** page will appear as shown on the right.

Repeat Step 4 if you need to add more clients or to configure more groups.

The screenshot shows the 'Mac address list' page. It has a title bar 'Mac address list'. Below it, there are four groups: Group1, Group2, Group3, and Group4. Each group has a checkbox and a dropdown menu. Group1 is selected, and its dropdown shows 'aa-bb-cc-dd-ee-ff'. Below the groups, there is a table with three rows of MAC addresses: 'ac-ec-fe-e3-34-56', '11-22-33-44-55-66', and 'be-ef-ba-ff-e1-11'. The second row is highlighted, and a mouse cursor is pointing at it.

7

This **Delete MAC Address** screen will appear to confirm whether you want to delete the selected client.

If you do not want to delete the client:

Click on the **Apply** button.

If you want to remove the client from the group:

Click on the **Delete** button.

The screenshot shows the 'Mac address list' page. It has a title bar 'Mac address list'. Below it, there is a single group selection: 'Group1' with a checkbox and a dropdown menu showing 'aa-bb-cc-dd-ee-ff'.

6

If you want to delete a particular client from a group:

1. Select the client to delete from the **Mac Address List**.

We illustrate with **11:22:33:44:55:66** from Group ID **4**.

2. Click on the **Delete** button.

The screenshot shows the 'Delete MAC address' screen. It has a title bar 'Delete MAC address'. Below it, there is a 'GroupID' dropdown menu showing '4'. Below that is an 'Apply' button. Below the button is a 'Mac Addr' dropdown menu showing 'ac-ec-fe-e3-34-56'. Below the dropdown is a 'Delete' button, which is highlighted by a mouse cursor.

Tag VLAN

While a port-based VLAN is limited in size since it can only exist within the confines of a single Ethernet switch, a Tag VLAN is designed to extend the wired VLAN to individual wireless clients.

Each VLAN is identified by a ‘tag’ which the switch associates with specific ports to which users are connected. Switches will pass this tag information with every data packet transmitted. Hence by using the same tag on each access point in the network, full client roaming can be supported while still guaranteeing the VLAN integrity.

The following steps show how to set up the *Tag VLAN* mode.

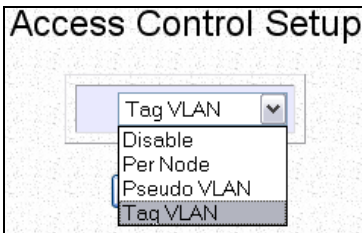
Wireless Pseudo VLAN

Tag VLAN:

expert

- 1 Click on the **Access Control** button.

The Access Control Setup menu shown on the right will appear.



- 2 The Wireless Pseudo VLAN function is *Disabled* by default.

1. Select **Tag VLAN** from the drop-down list.
2. Click on the **Apply** button.

Access control changed to TagVLAN will appear in the Message Window and the page shown in Step 3 will appear.

3

The **Tag VLAN** page enables you to manage specific VLAN groups by adding or deleting clients through their MAC address.

Click on the **Add** button.

	VLAN ID	Mac address list
Group1	☐ 1	
Group2	☐ 2	
Group3	☐ 3	
Group4	☐ 4	
Guest domain	☐ 5	

Add Delete

Apply Help

Add MAC address

GroupID 1 Mac Addr aa:bb:cc:dd:ee:ff

1 2 3 4

Cancel Help

4

1. Select a group number from the **Group ID** drop-down list.

We illustrate with Group ID **1**.

2. Fill in the **Mac Addr** field with the MAC address of the client in the format **xx:xx:xx:xx:xx**, where x is any value between 0-9 or a-f.

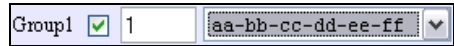
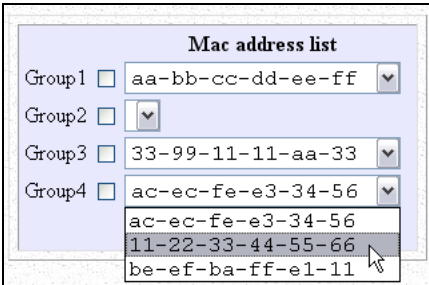
We illustrate with **aa:bb:cc:dd:ee:ff**.

3. Click on the **Apply** button.

You can also opt to add a client to the **Guest Domain**, in which case, it will be allowed to access the wired network resource though it will not be able to communicate with any other client in the other groups.

- 5** The updated **Mac Address List** page will appear as shown on the right.

Repeat Step 4 if you need to add more clients or to configure more groups.

- 6** If you want to delete a particular client from a group:

1. Select the client to delete from the **Mac Address List**.

We illustrate with **11:22:33:44:55:66** from Group ID **4**.

2. Click on the **Delete** button.

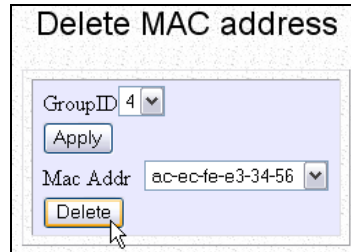
- 7** This **Delete MAC Address** screen will appear to confirm whether you want to delete the selected client.

If you do not want to delete the client:

Click on the **Apply** button.

If you want to remove the client from the group:

Click on the **Delete** button.



NAT

This section illustrates how you can host Internet servers on your LAN through the WPE54G configuration interface.

As a preliminary measure, you should ensure that the WPE54G is ready for basic Internet access on the LAN. The Network Address Translation (NAT) functionality is enabled by default in the WPE54G.

NAT functions by transforming the private IP address of packets originating from hosts on the LAN to appear as coming from a single public IP address and by restoring the destination public IP address to the appropriate private IP address for packets entering the private network. The multiple PCs on your LAN would then appear as a single PC to the WAN interface. The NAT firewall thus prevents unauthorised requests from the Internet from passing through the WPE54G, thereby protecting your LAN more effectively.

Using NAT, you can host a Virtual Server on the LAN. The implementation of a Virtual Server would enable you to host Internet servers such as a Web server, an FTP server or a Mail server on your network.

The De-Militarised Zone (DMZ) Host

The following acts as a guideline in configuring a DMZ Host.

Configuring a De-Militarised Zone (DMZ) Host

expert

1. Click on **NAT** from the **Configuration** menu.

The **Advanced NAT Options** are displayed near the bottom of the page. NAT is enabled by default.

2. Ensure that NAT is enabled before clicking on the **Apply** button.
3. Click on the **DMZ** button to configure Virtual Servers based on a De-Militarised Zone host.



2. Key in the IP address of the PC you wish to place within the DMZ in the **Private IP Address** field.

The default **Private IP Address** is set to 0.0.0.0. For illustration, we entered **192.168.168.55**

2. Click on the **Apply** button to effect the change.

3. To disable DMZ, enter **0.0.0.0** as the **Private IP Address**.
2. Click on the **Apply** button to effect the change.



The Port-Forwarding Virtual Server

Port forwarding redirects any incoming Internet request bearing a public IP address to another PC holding a private IP, based on its TCP/UDP port number.

Follow the steps shown to configure the Port Forwarding function.

Configuring a Port-Forwarding Virtual Server with WPE54G

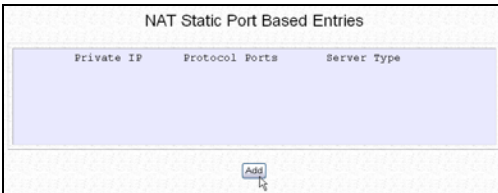
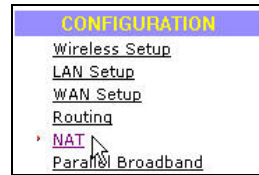
expert

1. Click on **NAT** from the **Configuration** menu.

The **Advanced NAT Options** are displayed near the bottom of the page.

NAT is enabled by default.

2. Ensure that NAT is enabled before clicking on the **Apply** button.
3. Click on the **Port Forwarding** button to display the **NAT Static Port Based Entries** GUI shown below.



2

- Click on the **Add** button.

This will bring up the **Add New NAT Port-Based Entry** GUI as shown below left.

3

1. Enter the relevant parameters.

To implement NAT, you have to specify the **Private IP Address** and **Server Type** of the Virtual Server in the **Known Server** section.

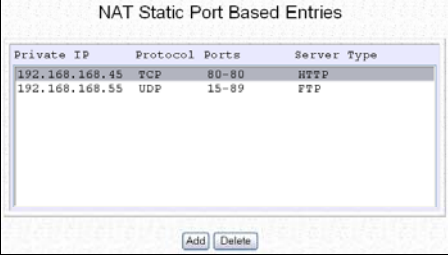
For the illustration above right, we entered **192.168.168.45** as the **Private IP Address** and selected **FTP** Server Type from the drop-down list.

However, for Internet applications not defined in the Known Server section, you will have to define the **Private IP Address**, the **Ports**, the **Protocol** and the **Server Type** in the **Custom Server** section.

For the illustration below right, we entered **192.168.168.55** as the **Private IP Address**, **15** till **89** as the selected **Ports**, **FTP** as the **Server Type** and selected **UDP** from the **Protocol** drop-down list.

2. Click on the **Add** button to add the address you have entered to the Port-based mapping table.

This will bring you to the screen illustrated in Step 4.



Private IP	Protocol	Ports	Server Type
192.168.168.45	TCP	80-80	HTTP
192.168.168.55	UDP	15-89	FTP

Add Delete

4

If you want to assign more PCs in your LAN as servers:

1. Click on the **Add** button.

This will bring you back to **Add New NAT Port-Based Entry** GUI.

2. Repeat Step 3.

If you want to delete any of the table entries:

1. Select the particular entry to delete.
2. Click on the **Delete** button.
3. The entry will disappear from the **NAT Static Port-Based Entries** table and **NAT port based entry deleted** will appear in the Message Window.

The IP-Forwarding Virtual Server

If you have subscribed for more than one IP address from your ISP, you may define Virtual Servers based on IP forwarding so that all Internet requests, regardless of the ports, are forwarded to specific computers within the private network.

Follow these steps to configure an IP-Forwarding Virtual Server.

Configuring an IP-Forwarding Virtual Server with WPE54G

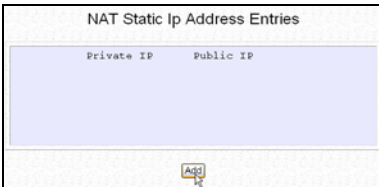
expert

1. Click on **NAT** from the **Configuration** menu.

The **Advanced NAT Options** are displayed near the bottom of the page NAT is enabled by default.



2. Ensure that NAT is enabled before clicking on the **Apply** button.
3. Click on the **IP Forwarding** button.



2

Click on the **Add** button.

3

1. Specify the **Private IP Address** and the **Public Address**.

For illustration, we determined all requests to public address **213.18.213.101** to be forwarded to a PC with private address **192.168.168.55**

2. Click on the **Add** button to proceed.



IP Forward Entries	
Private IP	Public IP
192.168.168.55	213.18.213.101
Add Back	

4

The **IP Forward Entries** table will reflect your new addition.



NOTE: For step 3 above, please ensure that you have subscribed to the public IP address you intend to forward from.

Routing

You can choose to configure the WPE54G with either Dynamic or Static Routing Protocol.

In Dynamic Routing, the Routing Information Protocol (RIP) will receive routing information from other routers on the network. In dynamic routing mode, RIP1 and RIP2 are chosen when there are multiple routes within your network. The broadband Internet Gateway will continuously update its routing table with the latest routing information by automatically adjusting to any physical changes in the network connection.

Follow the next steps to configure the IP Route Table.

Configuring the Routing Setup

IP Route Table:

1

Click on **Routing** from the **Configuration** menu.

This will bring you to the screen illustrated below right.

CONFIGURATION

- [Mode Selection](#)
- [Management Port](#)
- [WAN Setup](#)
- [NAT](#)
- [Routing](#)
- [IP Filtering](#)
- [SNMP Setup](#)
- [Remote Management](#)

IP Routing Table

Destination	Gateway
192.168.168.0	192.168.168.1
192.168.168.2	192.168.168.1
127.0.0.1	127.0.0.1
192.168.88.45	192.168.168.2

Dynamic Routing

Routing Protocol

Add IP Route

Destination IP Address	192	168	168	81
Gateway IP Address	192	168	168	2

IP Routing Table

Destination	Gateway
192.168.168.0	192.168.168.1
192.168.168.2	192.168.168.1
127.0.0.1	127.0.0.1
192.168.88.45	192.168.168.2
192.168.168.81	192.168.168.2

2

If you want to add a static route in the **IP Routing Table**:

Click on the **Add** button.

This will bring you back to **Add IP Route** GUI shown above left.

For illustration, we entered **192.168.168.81** as the **Destination IP Address** and **192.168.168.2** as the **Gateway IP Address**.

The new entry will appear in the updated **IP Routing Table** page as in the illustration below left and **Ip route entry added successfully** will appear in the Message Window.

3

If you want to delete any of the **IP Routing Table** entries:

1. Select the particular entry to delete.
2. Click on the **Delete** button.

The entry will disappear from the **IP Routing Table** and **Ip route entry deleted successfully** will appear in the Message Window.

IP Routing Table

Destination	Gateway
192.168.168.0	192.168.168.1
192.168.168.2	192.168.168.1
127.0.0.1	127.0.0.1
192.168.88.45	192.168.168.2
192.168.168.81	192.168.168.2

Dynamic Routing

In Dynamic Routing, the Routing Information Protocol (RIP) will receive routing information from other routers on the network. In dynamic routing mode, RP1 and RIP2 are chosen when there are multiple routes within your network. The broadband Internet Gateway will continuously update its routing table with the latest routing information by automatically adjusting to any physical changes in the network connection.

The next steps will guide you in setting up Dynamic Routing.

Configuring the Routing Setup

Dynamic Routing:

expert

1

Click on **Routing** from the **Configuration** menu.

This will bring you to the screen illustrated below right.

Dynamic Routing is set to **Disabled** by default.

CONFIGURATION

Mode Selection
Management Port
WAN Setup
NAT
▶ Routing
IP Filtering
SNMP Setup
Remote Management

IP Routing Table

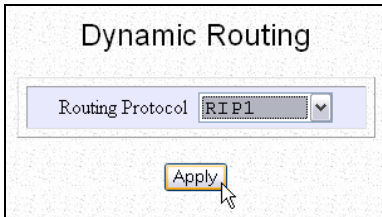
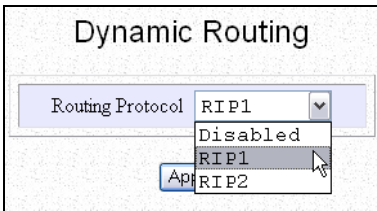
Destination	Gateway
192.168.168.0	192.168.168.1
192.168.168.2	192.168.168.1
127.0.0.1	127.0.0.1
192.168.88.45	192.168.168.2

Add Delete

Dynamic Routing

Routing Protocol Disabled ▼

Apply



2

If you want to enable Dynamic Routing:

1. Select your required protocol from the **Routing Protocol** drop-down list.
2. Click on the **Apply** button to save the changes made.

Applied parameter accepted. Please reboot the router for the settings to take effect will appear in the Message Window.

3. Reboot the system for the changes to take effect.

IP Filtering

When the IP Filtering functionality is enabled, the WPE54G will examine all outgoing packets before deciding, according to predefined rules, whether to block them or to let them pass.

The next steps will guide you through the IP Filtering setup.

Configuring the IP Filtering Setup

expert

1

1. Click on **IP Filtering** from the **Configuration** menu.

This will bring you to the middle screen illustrated on the right.

2. Click on the **Add** button to set a new rule to the **IP Filter Configuration**.

This will bring you to the screen illustrated below right.

CONFIGURATION

- Mode Selection
- Management Port
- WAN Setup
- NAT
- Routing
- ▶ **IP Filtering**
- SNMP Setup
- Remote Management

Filtering Configuration

Warning: Incorrect configuration may cause undesirable behavior.

All IP packets will be ☒ sent ☐ discarded, except for those matching one or more of the following

Select to Edit	Rule Name	IP Address(es)	Destination Port(s)	Day of the Week	Time of the Day
☐					

If the system loses its time settings, ☒ ignore ☐ accept the access time settings in the above rules

Apply Add Delete Edit Help

IP Filter Configuration

Add a new rule

Rule Name

IP Address Any

(From) 192.168.168.

(To) 192.168.168.

Destination Port Any

(From)

(To)

Day of the Week Any

(From) Sun

(To) Sun

Time of the Day Any (hh: 00-23, mm: 00-59)

(From) (hh:mm)

(To) (hh:mm)

Apply Cancel Help

2

1. Enter the relevant parameters.

(a). Rule Name

Rule Name	FTP_LAN3
-----------	----------

(b). IP Address

IP Address (From)	Any	▼
(To)	Any	▼
Range of IP Address:		
IP Address	Range	▼
(From)	192.168.168.23	
(To)	192.168.168.63	
Single IP Address:		
IP Address	Single	▼
(From)	192.168.168.23	
(To)	192.168.168.	
Any IP Address:		
IP Address	Any	▼
(From)	192.168.168.	
(To)	192.168.168.	

(c). Destination Port

Destination Port (From)	Any	▼
(To)	Any	▼
Range of Destination Ports:		
Destination Port	Range	▼
(From)	13	
(To)	89	
Single Destination Port:		
Destination Port	Single	▼
(From)	13	
(To)		
Any Destination Port:		
Destination Port	Any	▼
(From)		
(To)		

(a). For illustration, we entered **FTP_LAN3** as the **Rule Name**.

(b). From the **IP Address** drop-down list, select to apply the rule to a **Range** of IP addresses or to a **Single** IP address or to **Any** IP address.

For a **Range** of **IP Address**, key in **From** which IP address **To** which IP address. We illustrate from **192.168.168.23** to **192.168.168.23**.

For a **Single IP Address**, key in the address in the **From** field only. We illustrate with **192.168.168.23**.

No entry is required in either the **From** or **To** field if you selected **Any IP Address**.

(c). From the **Destination Port** drop-down list, select to apply the rule to a **Range** of port numbers or to a **Single** port number or to **Any** port numbers.

For a **Range** of **Destination Port**, key in **From** which port number **To** which port number. We illustrate from port number **13** to port number **89**.

For a **Single Destination Port**, key in the port number in the **From** field only. We illustrate with **13**.

No entry is required in either the **From** or **To** field if you selected **Any Destination Port**.

(d). Day of the Week

Day of the Week	Any
(From)	Any
(To)	Range
	Sun

Range of Days:

Day of the Week	Range
(From)	Mon
(To)	Mon

Single Day:

Day of the Week	Range
(From)	Mon
(To)	Mon

Any Day:

Day of the Week	Any
(From)	Sun
(To)	Sun

(d). From the **Day of the Week** drop-down list, select to apply the rule to **Any** day or to a specific **Range** of days.

For a **Range** of **Day**, select the days from the **From** and the **To** drop-down lists. We illustrate from **Monday to Friday**.

If you want the rule to apply for a single day, select a **Range** of **Day** and insert the same value in the **From** and **To** fields. We illustrate with **Monday to Monday**.

Leave the default in the **From** and **To** fields if you selected **Any Day**.

(e). Time of the Day

Time of the Day	Any
(From)	Any
(To)	Range
	(hh:mm)

Range of Time:

Time of the Day	Range
(From)	08:00 (hh:mm)
(To)	23:00 (hh:mm)

Any Time:

Time of the Day	Any
(From)	(hh:mm)
(To)	(hh:mm)

(e). From the **Time of the Day** drop-down list, select to apply the rule to **Any** time or to a specific **Range** of time.

For a **Range** of **Time**, key in **From** which time **To** which time.

The time entered should follow the 24H format, i.e. from 00:00 to 23:59.

We illustrate with **08:00 to 23:00**.

No entry is required in either the **From** or **To** field if you selected **Any Time**.

Apply	Cancel	Help
-------	--------	------

2. Click on the **Apply** button to save the changes made.

3 The new entry will appear in the updated **Filtering Configuration** table as illustrated on the right.

If the **Sent** radio button is enabled, all the outgoing packets will be sent except for those defined by the rule. Else, all outgoing packets will be blocked except for those defined by the rule.

For illustration, since the **Sent** radio button is enabled, the **FTP_LAN3** rule implies that all outgoing packets from IP address 192.168.168.23 to destination ports 13 to 27 will not go through at any time on any day.

1. If you want to save any changes made at this stage:

Click on the **Apply** button.

2. If you want to set another new rule to the **IP Filter Configuration**:

Click on the **Add** button and repeat Step 2.

3. If you want to delete any of the rules:

(a). Enable the **Select to Edit** radio button for the rule to delete as shown below right.

(b). Click on the **Delete** button.

4. If you want to edit any rule:

(a). Enable the **Select to Edit** radio button for the rule to edit as illustrated below right.

(b). Click on the **Edit** button.

Filtering Configuration

Warning: Incorrect configuration may cause undesirable behavior.

All IP packets will be ☒ sent ☐ discarded except for those matching one or more of the following rules.

Select to Edit	Rule Name	IP Address (s)	Destination Port(s)	Day of the Week	Time of the Day
☐	FTP_LAN3	192.168.168.23	13-27	Any	Any

If the system loses its time settings, ☒ ignore ☐ accept the access time settings in the above rules.

Filtering Configuration

Warning: Incorrect configuration may cause undesirable behavior.

All IP packets will be ☐ sent ☒ discarded except for those matching one or more of the following rules.

Select to Edit	Rule Name	IP Address (s)	Destination Port(s)	Day of the Week	Time of the Day
☒	FTP_LAN3	192.168.168.23	13-27	Any	Any

If the system loses its time settings, ☐ ignore ☒ accept the access time settings in the above rules.

Remote Management

This feature is especially helpful for those who work away from the office or from home. You only require Internet access to be able to manage your network.

Follow these steps to configure the Remote Management function.

Configuring the Remote Management Setup

expert**1**

Click on **Remote Management** from the **Configuration** menu.

This will bring up the screen shown below.

CONFIGURATION

[Mode Selection](#)
[uConfig IP Setup](#)
[Management Port](#)
[WAN Setup](#)
[NAT](#)
[Routing](#)
[IP Filtering](#)
[SNMP Setup](#)
▶ [Remote Management](#)

Remote Management

HTTP Port	80	(Standard=80)
TELNET Port	23	(Standard=23)

(Enter 0 to disable remote management)

Note: Changes made will only take effect after rebooting.

2

1. Specify the **HTTP Port** number and the **Telnet Port** number.

A standard entry for **HTTP port** is **80** while for **Telnet port**, it would be **23**.

2. Click on the **Save** button to save the changes made.
3. Click on the **Reboot** button to restart your computer so that the changes can take effect.

3

If you want to disable the **Remote Management** function:

1. Key in 0 in both the **HTTP Port** and the **TELNET Port**.
2. Click on the **Save** button to save the changes made.
3. Click on the **Reboot** button to restart your computer so that the changes can take effect.

Remote Management

HTTP Port (Standard=80)

TELNET Port (Standard=23)

(Enter 0 to disable remote management)

Note: Changes made will only take effect after rebooting.

Scan for Site Survey

This feature is available in all WPE54G modes. However the data captured when the WPE54G is in **AP mode** differs from that depicted when it is in **wireless client mode**.

Data collected in **AP mode**

- **Channel** refers to the channel that the WPE54G is using for transmission.
- **Interference** indicates the level of noise experienced by your WPE54G in terms of percentage of signal strength perceived from other access points within the network
- **Recommendation** can take three forms:
 - *Avoid* this channel since it is already being used by another device,
 - *Acceptable* if the noise level generated by other channels does not hinder communication in this channel,
 - *Recommended* if the noise level in this channel is negligible.

Data collected in **wireless client mode**

- When a WPE54G is connected to wired network and a set of wireless stations, it is referred to as a **Basic Service Set (BSS)**. The MAC address of the WPE54G is used as entry here.
- **SSID** refers to the network name which uniquely identifies the network to which the WPE54G is connected.
- **Ch** refers to the channel being used for transmission.
- **WEP** encryption can be enabled (**Y**) or disabled (**N**).
- **Signal** describes the strength of the signal received in percentage.

These steps illustrate how to use the Scan feature.

The Scan feature

- 1** Click on the **Scan** button to see the information collected.



Site Survey

BSS	SSID	Ch	WEP	Signal
☐ 000376d0011c	NP18 AG Network	11	N	70%
☐ 008048cb3878	wpe54g	6	N	71%
☐ 0080482776ba	ag	3	N	68%
☐ 0080482703d2	ts-compex26	3	Y	65%
☒ 0080482704b0	compex	6	N	66%
☐ 0230cd00000f	conexant	6	N	67%

- 2** In **wireless client mode**:
The **Site Survey** provides a list of the *BSS's* and *SSID's* available, the *channels* being used, whether *WEP* encryption is employed and the strength of the *signals* received.

To configure to a different SSID:

1. Select the radio button corresponding to the SSID you want to configure to.
2. Click on the **Apply** button to effect the change and return to the Setup page.

In **AP mode**:

The **Scan Status** page summarises the *channels* available, the level of *interference* and a *recommendation* concerning the usage of the respective channels.

If you want to use a different channel:

1. Select the radio button corresponding to the channel to configure to.
2. Click on the **Apply** button to effect the change and return to the Setup page.

In both cases, if you want to refresh the information displayed:

Click on the **Refresh** button.

Scan Status

Channel	Interference	Recommendation
☐ 1	0%	Recommended
☐ 2	0%	Acceptable
☐ 3	0%	Acceptable
☐ 4	0%	Acceptable
☐ 5	0%	Acceptable
☐ 6	66%	Avoid
☐ 7	0%	Acceptable
☐ 8	0%	Acceptable
☐ 9	0%	Acceptable
☒ 10	69%	Avoid
☐ 11	67%	Avoid
☐ 12	0%	Acceptable
☐ 13	68%	Avoid

Appendix A: Configuring for network access

This section illustrates how to configure your computer to communicate with the WPE54G.

Adding TCP/IP network protocol for Microsoft Windows 98/98SE/ME

To begin with, you have to ensure that your computer gets an IP address which it can use to communicate with the router or with other computers across your network.



NOTE: By default, the TCP/IP protocol is installed and set to obtain an IP address automatically in Windows 98, 2K & XP.

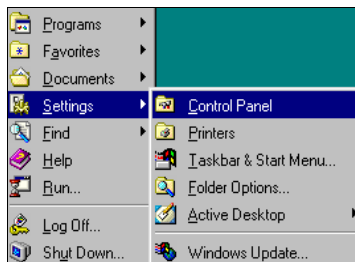
However, if your PC does not have TCP/IP installed, the following will guide you through the TCP/IP installation procedure.

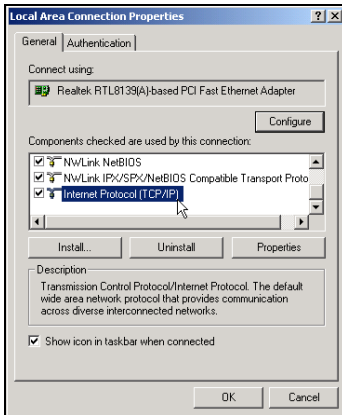
Adding TCP/IP protocol

Microsoft Windows 98/98SE/ME:

1

1. Click on **Start**.
2. Select **Settings**.
3. Click on **Control Panel**.





2

Double-click on the **Network** icon.

The **Network** Configuration screen shown on the left will appear.

3

Check your list of **Network Components** in the Network window's **Configuration** tab.

If TCP/IP is not installed:

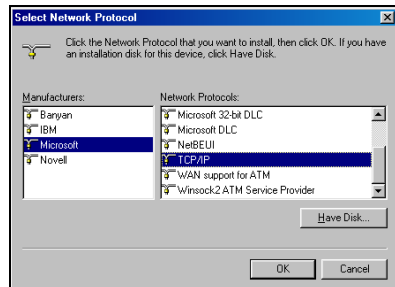
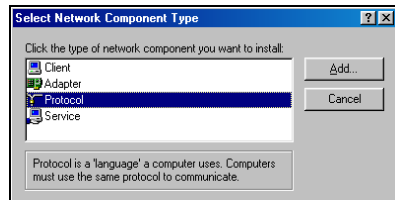
1. Click on the **Add** button.

This will bring you to the screen shown on the right.

2. Select **Protocol**.
3. Click on the **Add** button.

On the next screen that appears:

4. Select **Microsoft** from the **Manufacturers** column.
5. Choose **TCP/IP** from the **Network Protocols** column.



Configuring Dynamic IP address allocation

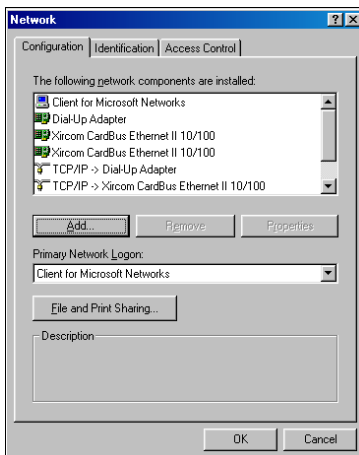
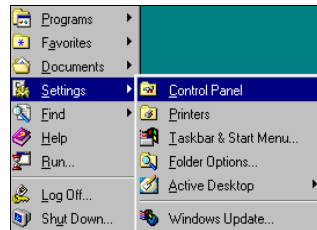
Microsoft Windows 98/98SE/ME

Follow these steps to configure Dynamic IP address allocation in your PC.

Configuring Dynamic IP address allocation

Microsoft Windows 98/98SE/ME:

1. Click on **Start**.
2. Select **Settings**.
3. Click on **Control Panel**.



2

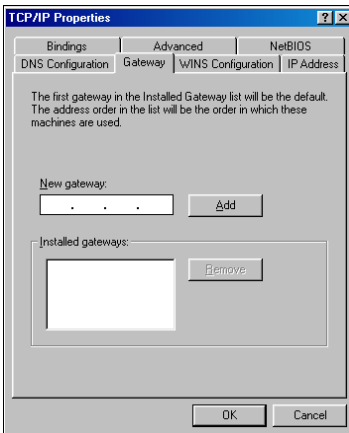
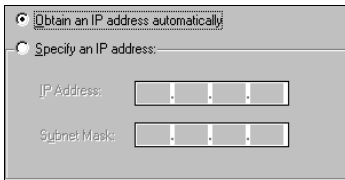
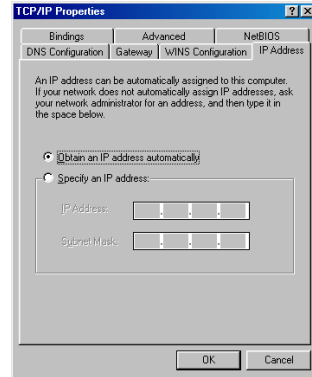
Double-click on the **Network** icon.

The **Network** configuration screen shown on the left will appear.

3

1. In the Network window's **Configuration** tab, select the TCP/IP component corresponding to your Ethernet adapter.
2. Click on the **Properties** button.

This will bring you to the screen shown on the right.

**4**

1. Click on the **IP Address** tab.
2. Enable the **Obtain an IP address automatically** radio button.
3. Click on the **Gateway** tab.
4. Verify that the **Installed Gateways** list is blank.
5. Click on the **OK** button.
6. Click on the **OK** button.

This will return you to the **Network** dialog page.



NOTE: Windows may ask you for the original Windows installation disk or additional files. Check for the files at **C:\windows\options\cabs**, or insert the Windows CDROM disc into the CDROM drive and search for the appropriate files.

Configuring Static IP address allocation

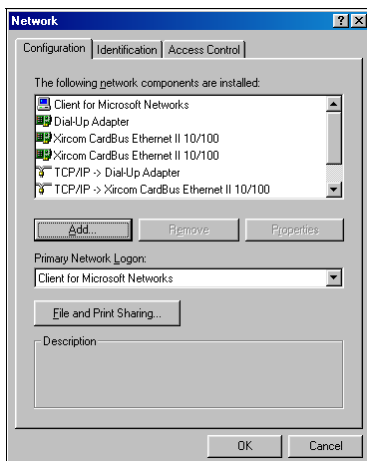
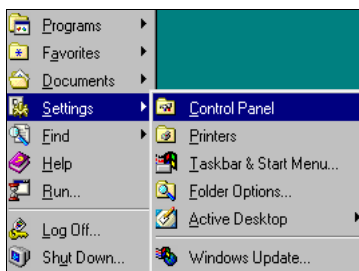
Microsoft Windows 98/98SE/ME

The following will help you configure your PC with Static IP address allocation.

Configuring Static IP address allocation

Microsoft Windows 98/98SE/ME:

1. Click on **Start**.
2. Select **Settings**.
3. Click on **Control Panel**.



2

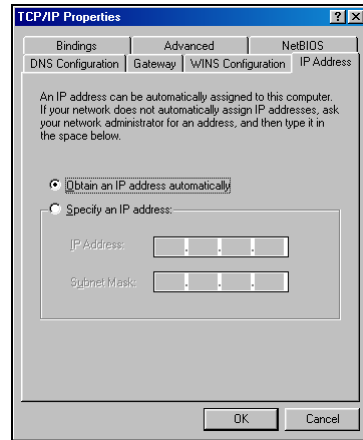
Double-click on the **Network** icon.

The **Network** Configuration screen shown on the left will appear.

3

1. In the Network window's **Configuration** tab, select the TCP/IP component corresponding to your Ethernet adapter.
2. Click on the **Properties** button.

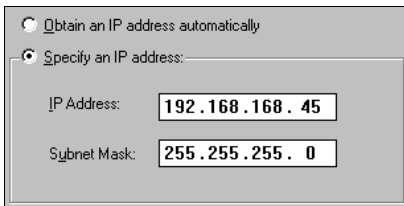
This will bring you to the screen shown on the right.

**4**

1. Click on the **IP Address** tab.
2. Enable the **Specify an IP address** radio button.
3. Fill in the **IP Address** field as **192.168.168.X**, where X is any value from 2 to 254.

For illustration, we keyed in **192.168.168.45** as IP address.

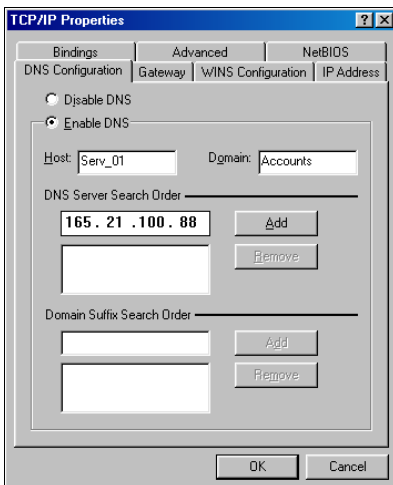
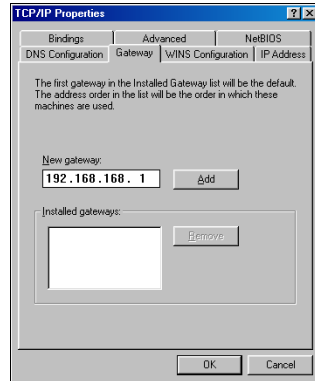
4. Key in **255.255.255.0** as the **Subnet Mask**.



5. Click on the **Gateway** tab.
2. Key in the IP address of the WPE54G in the **New Gateway** field.

The default IP address of the WPE54G is 192.168.168.1 as we illustrate on the right.

3. Click on the **Add** button.



6. Click on the **DNS Configuration** tab.
2. Select the **Enable DNS** radio button.
3. Type in a unique identifying name in the **Host** field.

We illustrate on the left with **Serv_01**.

4. Key in the IP address of your DNS server, as specified by your Internet Service Provider in the **DNS Server Search Order** field.
5. Click on the **Add** button.
6. Click on the **OK** button.
7. Restart your computer for the changes to take effect.

Configuring Wireless Network Settings

It is usually recommended to configure the wireless client PC or notebook with automatic IP addressing.

Microsoft Windows XP

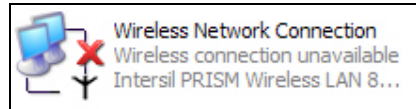
These steps will guide you in configuring your wireless network settings.

Configuring Wireless network settings

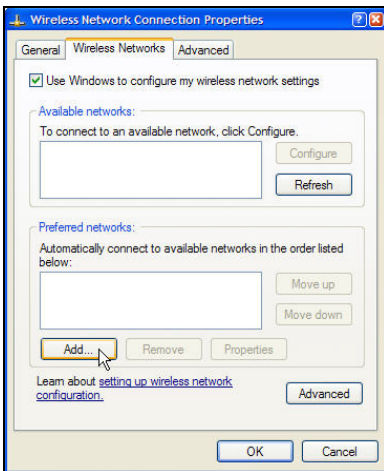
Microsoft Windows XP:

1

1. Right-click on **Wireless Network Connection** corresponding to the wireless Ethernet adapter that you wish to connect to the WPE54G.



2. Click on **Properties**.

**2**

1. Click on the **Wireless Network** tab.
2. Click on the **Add** button.

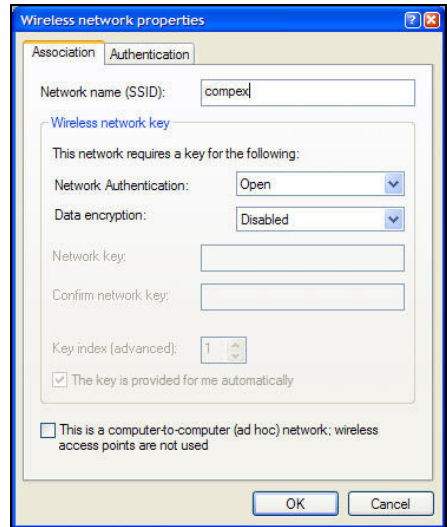
3

1. Key in the SSID of the wireless network in the **Network name** field.

Ensure that the ESSID entered is the same as that entered for the access point as well as all other clients within the same wireless network.

We illustrate with **compex** on the right.

2. Click on the **OK** button.
3. You can disconnect the Ethernet cable from your PC and connect it to the Fast Ethernet LAN you wish to bridge.



Appendix B: Troubleshooting

Solutions to Common Problems

In this section, we list suggested steps to follow in order to rectify certain common problems that may arise during the installation and operation of the NetPassage WPE54G. If you do not find an answer here, you may also visit the corporate Compex website at www.compex.com.sg or www.cpx.com.

1. I want to know whether the WPE54G is connected to the Internet.

A. Open a Command Prompt

- ◆ For Windows 98 and ME, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **command**. Press the **Enter** key or click the **OK** button.
- ◆ For Windows 2000 and XP, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **cmd**. Press the **Enter** key or click the **OK** button.

B. In the Command Prompt, type **ping 192.168.168.1** and press the **Enter** key.

- ◆ If you get a reply, the computer is communicating with the WPE54G.
- ◆ If you do NOT get a reply, please check the cables and ensure that the settings are correct before trying again.

C. In the Command Prompt, type **ping www.yahoo.com** and press the **Enter** key.

- ◆ Getting a reply means that the computer is connected to the Internet.
- ◆ Otherwise, you may want to ping another known host.
Getting no reply from any of the other hosts that you try, implies that the problem lies with your connection.

2. I am not getting an IP address on my connection and I am unable to surf the Internet.

- A. Make sure that the Ethernet cable is properly connected from your Cable/ADSL modem to the WPE54G's port, and verify from the **About System** page whether a valid IP address from the ISP is shown on the information page. Then refer to Problem 1 on page [84](#), and follow the steps A, B & C as described, to verify connectivity with the WPE54G.
- B. Ensure that you are using the appropriate WAN settings to suit your broadband connection. You may contact your ISP to enquire whether your Internet connection type should be Dynamic IP addressing or Static IP addressing, or whether it is PPPoE (commonly used for ADSL subscriptions). Please refer to *Chapter 6 – Advanced Configurations* on page [41](#) for WAN Setup.
- C. If you are able to surf the Internet when your Cable/ADSL modem is connected directly to your PC, and find that your NetPassage WPE54G is unable to get an IP address from the ISP even after going through steps A & B above, then you may need to clone the MAC address of your Ethernet adapter onto the WPE54G.
- D. If all configuration settings from points A to C above have been followed but in vain, power off the computer, the WPE54G and the Cable/ADSL modem. Turn on the Cable/ADSL modem then wait for 1 minute before turning on the WPE54G. Lastly, turn on your computer. Verify again whether you have been allocated an IP address and are able to surf the web.

3. I am not able to access the web-based configuration page of the NetPassage WPE54G

- A. Refer to Problem 1 on page [84](#), and first follow the steps described in that section to verify connectivity with the WPE54G.
- B. If you are a PPPoE user, you will need to remove the proxy settings or the dial-up pop-up window.
- ♦ For Microsoft Internet Explorer 5.0 or later versions, start Internet Explorer, from the **Tools** menu bar, select **Internet Options** and then click on the **Connections** tab.
 - From the **Connection** tab, click on the **LAN Settings** button. Uncheck any options from that dialog box. Press the **OK** button to return to the previous screen.
 - Click the radio box option **Never dial a connection** to remove any dial-up pop-ups for PPPoE users. Press the **OK** button to finish.
- ♦ For Netscape 4.7 or later versions, start Netscape Navigator. From the **Edit** menu bar, select **Preferences**, then **Advanced**, and finally **Proxies**.
 - Make sure that the **Direct connection to the Internet** option is selected.
 - Close all windows to finish.

4. I wish to start all over. I want to set the WPE54G to its factory default settings.

- A. In the event that you may wish to return the WPE54G to its original factory default settings, depress the Reset button (at the back of the router) when the router is powered up and hold it for 10 seconds before releasing it.

Appendix C: Frequently Asked Questions

Answers to Frequently Asked Questions

In the section, we have compiled a short list of answers to some frequently asked questions about the Compex NetPassage WPE54G product. If you cannot find an answer here, you may visit the corporate Compex website at www.compex.com.sg or www.cpx.com.

	Question	Answer
1.	Is IPSec passthrough supported by the WPE54G?	Yes. It is an automatically enabled feature supported by the WPE54G.
2.	Does the WPE54G support operating systems other than Windows 98, ME, 2000 and XP?	Yes. However, Compex does not provide technical support for the set up, configuration or troubleshooting of these non-Windows operating systems.
3.	What is the maximum number of IP addresses that the WPE54G can support?	The WPE54G will support up to 253 IP addresses.
4.	Does the WPE54G support 100Mbps Ethernet?	Yes. 100Mbps Ethernet is supported. However, your Internet connection speed will vary depending on the speed/type of broadband subscription.
5.	What is NAT and what is it used for?	Network Address Translation (NAT) multiplexes multiple private IP addresses for the LAN to a single public IP address on the Internet. <u>For more information on NAT, please refer to the NAT Technology Primer on the Product CD.</u>
6.	What is a MAC address?	MAC is the abbreviation for Media Access Control. The MAC address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter or router. It allows the network to identify the hardware. Unlike IP addresses, the MAC address is permanent and therefore constitutes a valuable identifier.
7.	What's the difference between Short and Long Preamble?	The preamble is part of the IEEE 802.11b physical layer specification, and specifically, part of the Physical Layer Convergence Protocol (PLCP). All 802.11b devices must support the long preamble format , but may optionally support the short preamble.

Appendix D: Glossary of Terms

10Base-T	An IEEE Ethernet standard for 10Mbps data transmission using unshielded twisted pair wires
100Base-Tx	An IEEE Ethernet standard for 100Mbps data transmission using two pairs of Category 5 UTP wire
802.11b	An IEEE standard for wireless networking standard specifying a maximum data transmission rate of 11Mbps using DSSS modulation and an operating frequency of 2.4GHz.
802.11g	A draft standard proposed by IEEE that is awaiting ratification, to be an extension of the IEEE 802.11 standard. It specifies a data transfer rate of 54Mbps using OFDM modulation and an operating frequency of 2.4GHz, as well as backward compatibility with the 802.11b devices.
Bit	Short for "Binary Digit." It uses 0 and 1 as the value for the binary numbering system. It is also the smallest form of data.
Broadcasting	To simultaneously send the same message to all network members.
Browser	The browser is a general name given to applications designed to view and interact with HTML pages on the World Wide Web.
CAT 5	It is a standard developed by the Electronics Industries Association that specifies network cabling which consists for twisted pairs of copper wire with a sustainable data rate of 100Mbps.
Database	A database is a collection of information that is organized so that the contents may be easily accessed/managed.
Data Packet	In an IP network, packet switching is the method employed to transmit data and the smallest chunk of data is called a packet (packet size can vary).
DHCP	Dynamic Host Configuration Protocol. It is a protocol that allows the network administrator to centrally manage and assign IP addresses to devices in the network. <u>For more information on DHCP, please refer to the DHCP Technology Primer found on the Product CD.</u>
DMZ	De-Militarized Zone hosting allows the administrator to expose a private IP address onto the Internet. It is used for a PC/Server assigned with a Static IP address which has to run specialized applications requiring multiple TCP/IP ports to be opened.
DNS	Domain Name System translates Internet domain names to IP addresses, giving meaningful and easy-to-remember names to otherwise arcane IP addresses.
Driver	A piece of software developed to interface a piece of hardware with

		its immediate upper-layer software (i.e. operating system) so that it can be recognized and operated.
DSSS		Direct Sequence Spread Spectrum is a modulation scheme employed by the 802.11b standard that uses a chipping code (redundant bit) during its transmission to reject interference.
Dynamic IP Address		It is an IP address that is dynamically allocated or assigned to a client device within a TCP/IP network, typically by a DHCP server.
EAP-MD5		EAP-MD5 lets a RADIUS server authenticate LAN stations by verifying an MD5 hash of each user's password. This is a simple and reasonable choice for trusted Ethernet networks where there is low risk of outsider sniffing or active attack. However, EAP-MD5 is not suitable for public Ethernet or wireless LANs because outsiders can easily sniff station identities and password hashes, or masquerade as access points to trick stations into authenticating with them instead of the real deal.
Encryption		Encryption is a security method applying specific algorithms to make sure that all the data from one computer is encoded into a form that only the other intended party will be able to decode and view the information.
Ethernet		An IEEE standard network protocol that specifies how data is transmitted over a common medium. It uses CSMA/CD which stands for Carrier Sense Multiple Access with Collision Detection. It has a defined data rate of 10Mbps.
Fast Ethernet		An IEEE standard extended from 10Base-T Ethernet to support 100Mbps data rate.
Firewall		It is a software layer that controls network access from within and without so that any undesired activity may be prevented by malicious or snooping parties.
Firmware		It is a software code written and saved within the read-only memory (ROM) or programmable read-only memory (PROM). The firmware that is written on the ROM/PROM is retained even when the device is powered off.
FTP		File Transfer Protocol. It is a protocol designed to transfer files over a TCP/IP network.
Full Duplex		It defines the ability of a device to transmit data simultaneously in both upstream and downstream directions over a single line.
Gateway		A gateway is a device that interconnects networks.
Half Duplex		It defines the ability of a device to transmit in one direction at a time over a single line.
HTTP		HyperText Transport Protocol is a common protocol used to connect servers on the World Wide Web, with its primary function being to establish a connection with a web server and transmit HTML pages to the client's browser.

ICMP	Internet Control Message Protocol is a message control and error reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.
IGMP	Internet Group Management Protocol is the standard for IP multicasting on the Internet. It is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group. All hosts conforming to level 2 of the IP multicasting specification require IGMP.
IEEE	It is the Institute of Electrical and Electronic Engineers. The IEEE is a professional technical body promoting the development and application of technology.
IP Address	At the moment, IP address is a 32-bit binary digit that defines each sender or receiver of information across an IP network.
IPSec	Internet Protocol Security. It is a suite of protocols used to implement secure exchange of packets at the IP layer.
ISP	Internet Service Provider. It is a company that provides individuals or corporations with Internet access and other related services.
LAN	Local Area Network is a group of computers and devices sharing a common communication medium within a small geographical area.
Latency	Latency is a time-delay.
MAC Address	MAC is the abbreviation for Media Access Control. The MAC address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter or router, that allows a network to identify the hardware. Unlike IP addresses, this number is permanent and is therefore a valuable identifier.
Mbps	Mega bits per second. It is a unit of measurement for data transmission indicating a million bits per second.
Multicasting	To transmit a single message to a select group of network recipients.
NAT	Network Address Translations multiplexes multiple private IP addresses for the LAN to a single public IP address on the Internet. <u>For more information on NAT, please refer to the NAT Technology Primer on the Product CD.</u>
OFDM	Orthogonal Frequency Division Multiplexing. It is a modulation scheme employed by the IEEE 802.11g standard, which combines numerous signals of different frequencies to form a single signal for transmission over a medium.
Packet Filtering	This is a means of discarding unwanted network traffic based on its originating addresses or the type of data transmitted.

Ping	Packet Internet Groper is a utility used to determine whether a particular IP address is available online. It works by sending out a packet and waiting for a response from the recipient.
PPPoE	Point-to-Point Protocol over Ethernet is a method for the encapsulation of PPP packets over Ethernet frames.
PPTP	Point-to-Point Tunneling Protocol supports the creation of Virtual Private Networks by ensuring that messages transmitted from one VPN node to another are secure. Users can use PPTP to dial in to their corporate network via the Internet.
Preamble	A preamble is a signal used in network communications to synchronize the transmission timing between two or more systems. Proper timing ensures that all systems are interpreting the start of the information transfer correctly.
RJ-45	A connector used for Ethernet devices which holds up to eight wires.
SNMP	Simple Network Management Protocol is a monitoring and controlling protocol. SNMP devices/applications report network activity within to a workstation console so that it may be monitored and controlled.
Subnet Mask	Subnet masking is a method of splitting IP networks into subgroups.
TCP	Transmission Control Protocol enables two hosts to establish a connection and exchange streams of data, guaranteeing delivery of data and that packets will be delivered in the same order in which they were sent.
Throughput	It is the measurable amount of data moved from one place to another within a given time period.
UDP	User Datagram Protocol is a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP provides a direct way to send and receive datagrams over an IP network and is used primarily for broadcasting messages over a network.
Unicasting	Communication that takes place over a network between a single sender and a single receiver.
URL	Uniform Resource Locator is the address that defines the location of a file on the World Wide Web.
UTP	Unshielded Twisted Pair is the most common kind of copper wiring designed to reduce crosstalk between copper wires.
VPN	Virtual Private Network is a secure means to join remote networks using comprehensive authentication and encryption. They may be "virtually" joined even across a public network like the Internet by means of employing IPSec amongst others.
WAN	Wide Area Network. It is a communication network that extends over a large geographical area.

WEP		Wired Equivalent Privacy is a wireless data privacy encryption protocol based on a 64-bit or 128-bit shared key algorithm.
WLAN		Wireless Local Area Network is a group of computers and associated devices that communicate with each other wirelessly.

Appendix E: Technical Specifications

Compex NetPassage WPE54G

Industry Standards	Wired: - IEEE 802.3 10Base-T - IEEE 802.3u 100Base-Tx - IEEE 802.3x Flow Control Wireless: - IEEE 802.11 DSSS - IEEE 802.11b - IEEE 802.11 OFDM - IEEE 802.11g
WAN Interface	1x RJ45 Ethernet LAN Port (for Cable/ADSL modem)
WAN Type	- Static IP - Dynamic IP - PPP over Ethernet (PPPoE) - PPTP
LAN/WLAN Interface	Wireless: - Operating channels, frequency of: 11 Channels 2.400~2.4835, US, Canada 13 Channels, 2.400~2.4970, Europe 4 Channels 2.400~2.4835, France - Wireless Distributed System (WDS) feature for wireless connection of further APs to extend the existing network. - Direct Sequence Spread Spectrum modulation, Orthogonal Frequency Division Multiplexing modulation - Data rates: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 11Mbps, 9Mbps, 6Mbps, 5.5Mbps, 2Mbps, 1Mbps

	- Security: • 64-bit/128-bit WEP • Wireless Pseudo VLAN • 802.1x (supports EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MD5, MAC address authentication) • Tag VLAN
IP Addressing	All Classful/Classless subnets
Built-in DHCP Server	Yes
DHCP Reservation	Yes
Load-Balancing/ Fail-Over Redundancy	Parallel Broadband
Virtual Server	IP and Port Forwarding, De-Militarized Zone hosting
IP Packet Filtering	Time-based, TCP Port, Source IP filtering
IP Routing	Static Routing Entry
VPN Client Pass-Through	PPTP, IPsec, L2TP
Configuration Interface	Web-based Configuration Menus
Profile Backup and Restore	Yes
Firmware Upgradeable	Yes
Environment Requirement	Temperature: - Operating : 0°C to 40°C - Storage : -20°C to 70°C Humidity: - Operating : 10% to 80% RH - Storage : 5% to 90% RH

Appendix F: Technical Support Information

The warranty information and registration form are found in the Quick Install Guide.

For technical support, you may contact Compex or its subsidiaries. For your convenience, you may also seek technical assistance from the local distributor, or from the authorized dealer/reseller that you have purchased this product from. For technical support by email, write to support@compex.com.sg.

Refer to the table below for the nearest Technical Support Centers.

Technical Support Centers	
Contact the technical support center that services your location.	
U.S.A., Canada, Latin America and South America	
 Write	Compex, Inc. 4051 E. La Palma, Unit A Anaheim, CA 92807, USA
 Call	Tel: +1 (714) 630-7302 (8 a.m.-5 p.m. Pacific time) Tel: +1 (800) 279-8891 (Ext.122 Technical Support)
 Fax	Fax: +1 (714) 630-6521 BBS: +1 (714) 630-2570 (24-hour access)
Europe	
 Write	ReadyLINK Netzwerktechnology Gmbh Albert Einstein Straße 34/M21 63322 Rödermark, Germany
 Call	Tel: +49 (0) 6074 - 98017 (8 a.m.-5 p.m. local time)
 Fax	Fax: +49 (0) 6074 - 90668 BBS: +49 (0) 6074 - 93974 (24-hour access) Support Email: readylink@compex.com.sg
Asia, Australia, New Zealand, Middle East and the rest of the World	
 Write	Compex Systems Pte Ltd 135, Joo Seng Road #08-01, PM Industrial Building Singapore 368363
 Call	Tel: (65) 6286-1805 (8 a.m.-5 p.m. local time) Tel: (65) 6286-2086 (Ext.199 Technical Support)
 Fax	Fax: (65) 6283-8337 BBS: (65) 6282-8854 (24-hour access)
Internet access/	
E-mail:	support@compex.com.sg
FTPsite:	ftp.compex.com.sg

Note:

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.