

Step 3:
Click the **Add** button to create the rule for LAN user's bandwidth control.

Add Bandwidth Control Entry

Bandwidth Control Rule

Rule Name :

Committed Rate(kbit) :

Ceil Rate(kbit) :

Rule type :

IP/MAC Address :

Parameters	Description
Rule Name	You can set a name for the bandwidth control rule.
Committed Rate (kbit)	Minimum bandwidth rate of throughput. NOTE: The sum of the Committed Rate of all the rules should not exceed the total rate available.
Ceiling Rate (kbit)	Capped bandwidth rate of throughput.
Rule Type	This defines whether the bandwidth control rule works on downloads or uploads, and whether it works by IP address or MAC address.
IP/MAC Address	IP address or MAC address for the bandwidth control rule, corresponding to whether the Rule Type is defined by IP address or MAC address.

Step 4:
Click the **Add** button.

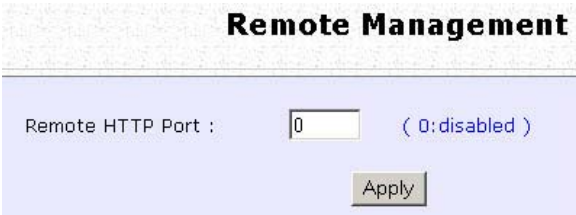
Repeat Steps 1 to Step 3 to add new bandwidth rule.

Perform Remote Management

(Available in Wireless Routing Client and Gateway modes)

You can use the access point web-based interface from the Internet to manage your network remotely.

Setup Remote Management




Step 1:
Select **Remote Management** from the **CONFIGURATION** command menu.

Step 2:
To disable Remote Management, set **Remote Http Port** to 0

To enable Remote Management, set **Remote Http Port** to an unused port number. It is recommended that you avoid using port number 80 as it is blocked by some ISPs.

In Gateway mode, **Remote Management** is enabled with Port 88 and the Ethernet port becomes a WAN port. To continue using it, open the web manager using the WAN IP with Port 88.
Example: For WAN IP 100.100.100.1 use `http://100.100.100.1:88`

NOTE



It is recommended that the default password is replaced with a new password changed periodically to prevent unauthorized access.

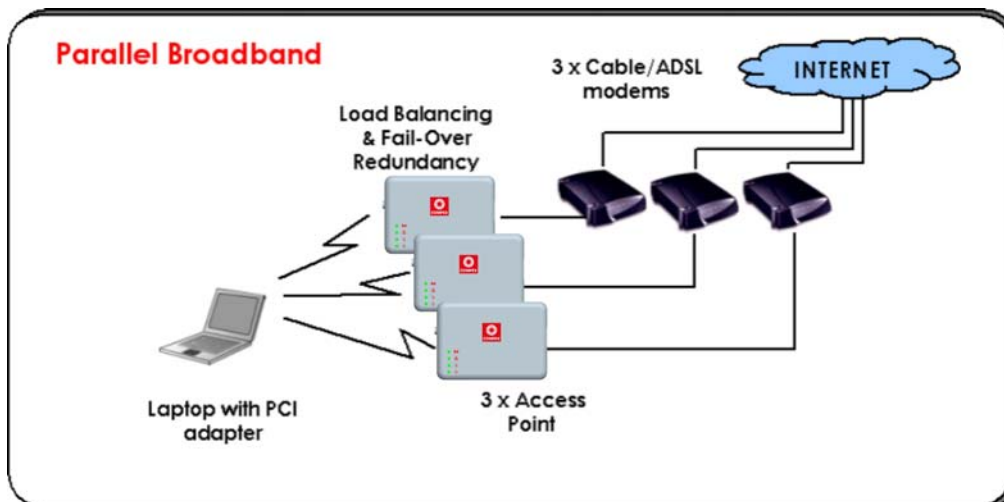
Use Parallel Broadband

(Available in Gateway mode)

Parallel Broadband provides scalable Internet bandwidth with Load Balancing and Fail-Over Redundancy.

Load Balancing is provided by balancing the aggregate bandwidth of multiple broadband connections across the traffic demands of your private network. With Parallel Broadband, if a particular broadband connection fails, the access point will use the remaining functional broadband connections, thus providing Fail-Over Redundancy.

Implementing Parallel Broadband requires the installation of 2 or more access points in the network, each connected to separate broadband Internet service account. As there is no restriction to the type of broadband Internet they are connected to, be it cable or ADSL, you may thus have one access point connected to cable Internet, and another to an ADSL line. The access points have to be operating in Gateway mode with Parallel Broadband and set to the same ESSID.



Enable Parallel Broadband

Begin by verifying that every access point in the network is properly configured to connect to its individual broadband Internet account.

Secondly ensure that either:

- each access point is connected to an Ethernet port in the network
OR
- the access points are wired to each other.

Then all the access points has to have the DHCP server, followed by the Parallel Broadband feature, enabled through the web-based configuration. Please note that all the access points need to be interconnected.

Step 1:
Select **Parallel Broadband** from the **CONFIGURATION** command menu.

Step 2:
Select **Enable** and click the **Apply** button.



Step 3:
Repeat Step 1 and Step 2 for the rest of the access points.

New users will then be assigned to the access point with the smallest load, ensuring that each access point has approximately the same number of users.

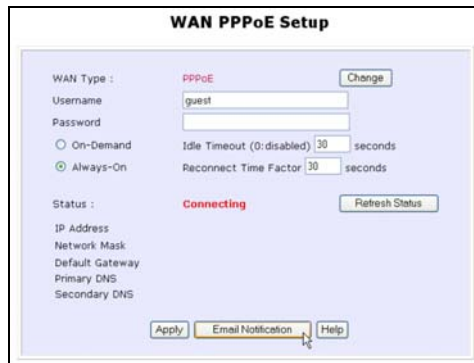


Important:

Implementing Parallel Broadband is redundant if there is only 1 access point.

Setup Email Notification

This feature notifies you by email if there is a change in the WAN IP address that was supplied to you.



Step 1:
Select **WAN PPPoE Setup** or **WAN PPTP Setup** from the **CONFIGURATION** command menu.

Step 2:
Click on the **Email Notification** button.



Step 3:
Select to **Enable** Email Notification and enter the following details:

- **Email address of Receiver:**
Email address of the receiver to whom the message would be sent.
- **IP address of Email Server:**
IP address of the SMTP server through which the message will be sent. It is recommended that you use your ISP's SMTP server.
- **User Name:**
User Name for the specified email account. This is necessary if authentication is required.
- **Password:**
Pass word for the specified email account. This is necessary if authentication is required.
- **Email address of Sender:**
Email address to be displayed as the sender.

Step 4:
Specify whether the SMTP server **Needs Authentication** or not by setting the checkbox accordingly. By default it is not selected.

Step 5:
Click on the **Apply** button.

Using Static Address Translation

(Available in Wireless Routing Client and Gateway modes)

If you use a notebook for work in the office, you most probably bring it home to connect to the Internet as well. Since it is most likely that your office network and home network broadband-sharing network subnets are configured differently, you would have the hassle of reconfiguring your TCP/IP settings every time you use the notebook in a different place. Static Address Translation allows you to bypass this hassle.

With SAT, if you try to access the Internet on your notebook from home but with your office TCP/IP settings, the notebook will try to contact the IP address of your office gateway to the Internet. When the access point finds that the notebook is trying to contact a device lying on a different subnet from that of the home network, it would inform the notebook that the gateway to the Internet is in fact the access point itself. From then the notebook would contact the access point for access to the Internet without any change to the TCP/IP settings.

NOTE



For SAT to function properly:

1. The IP address of the notebook should belong to a different subnet from the LAN IP address of your access point.
2. The <Default Gateway> in the TCP/IP settings of your notebook should NOT be left blank.

Step 1:

Select **Static Address Translation** from the **Home User Features** command menu.

Step 2:

Select whether to **Enable** or **Disable** SAT, and click the **Apply** button.

SAT is disabled by default.

A screenshot of a dialog box titled "Enable/Disable Static Address Translation". The dialog has a light blue background. At the top, the title is in bold black text. Below the title, there is a label "Status :" followed by two radio buttons. The first radio button is selected and is labeled "Enable". The second radio button is unselected and is labeled "Disable". At the bottom center of the dialog, there is a grey button labeled "Apply".

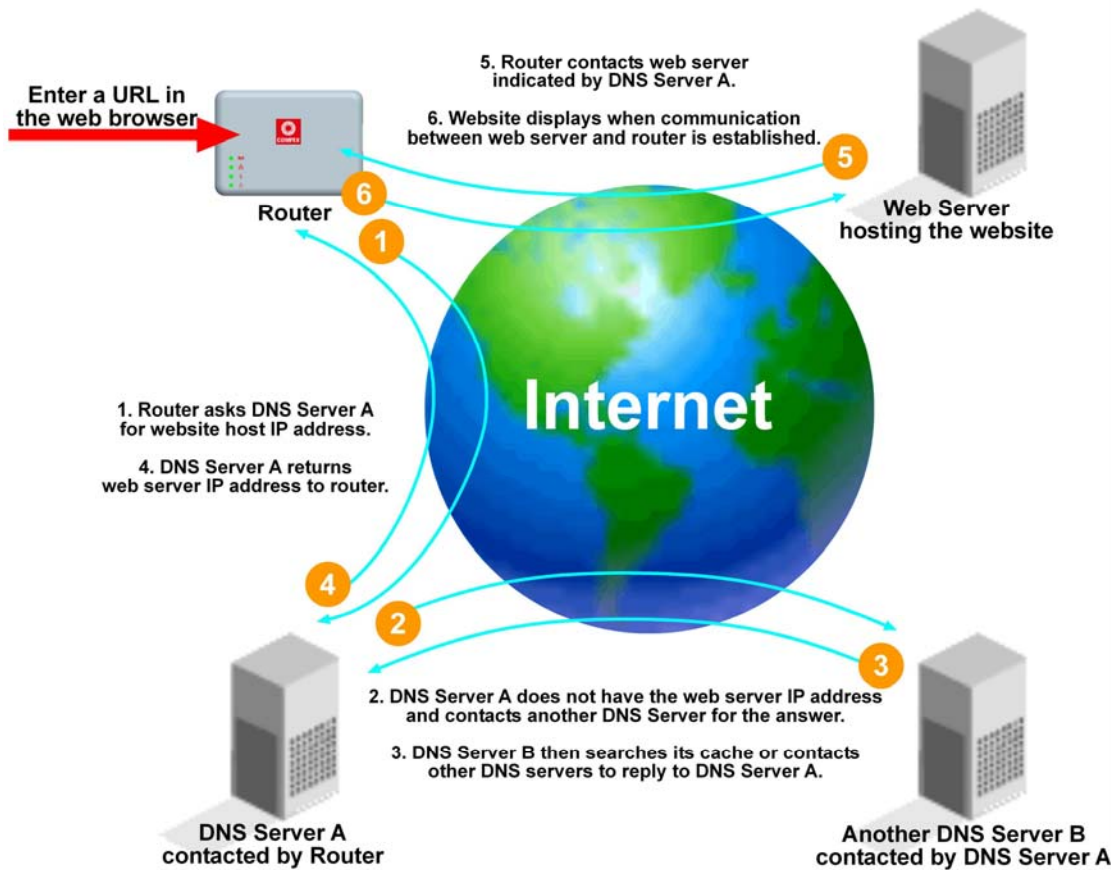
Use DNS Redirection

(Available in Wireless Routing Client and Gateway modes)

When you enter a URL into your Internet browser, it requests for a name-to-IP address translation from the Domain Name System (DNS) servers to locate the web server hosting the desired website. The DNS server searches its local cache for the answer, and if found, returns this cached IP address. Otherwise, it contacts other DNS servers until the query is answered.

With DNS Redirection, DNS requests from the LAN clients are processed by the access point. It contacts the DNS server allocated by your ISP to resolve these DNS requests unless you have already specified a default DNS server in the access point LAN Setup. This default DNS server overrides the one defined in the TCP/IP settings of the LAN clients, allowing the access point to direct DNS requests from the LAN to a local or to a closer DNS server that it is aware of, thus improving the response time.

DNS Redirection also provides more control to the network administrator. In the event that there is a change in DNS servers, he can simply indicate the actual DNS server IP address in the access point LAN Setup and enable DNS Redirection, without having to reconfigure the DNS settings of every LAN client.




NOTE



An entry for the DNS Server field in the PC TCP/IP Properties is required for Internet access. If the exact DNS IP address is unavailable, simple key in any valid IP address, for example:
10.10.10.10

Enable or Disable DNS Redirection

Step 1:
Select **DNS Redirection** from the **Home User Features** command menu.



Enable/Disable DNS Redirection

Status : Enable Disable

Apply

Step 2:
Select to **Enable** or **Disable** DNS Redirection.

Step 3:
Click the **Apply** button.

Dynamic DNS Setup

With Dynamic IP Internet connection, keeping track of your public IP address for Internet communication is complicated as it is changed regularly by the ISP. If you are doing some web hosting on your computer, Internet users will have to keep up with the changing IP address to access your computer.

When you sign up for an account with a Dynamic Domain Name Service (DDNS) provider, it will register your permanent domain name, for example: **MyName.Domain.com** You can configure the access point to automatically contact your DDNS provider whenever it detects a change in its public IP address. The access point will then log on to update your account with its latest public IP address.

If a user enters your address: **MyName.Domain.com** into their web browser, this request would go to the DDNS provider which will then redirect the request to your computer, regardless of the IP address it is currently assigned by your ISP.

To enable/disable Dynamic DNS Setup

Step 1:

Select **Dynamic DNS Setup** from the **Home User Features** command menu.

Step 2:

Select to **Enable** or **Disable** Dynamic DNS.

Dynamic DNS is disabled by default.

Click the **Apply** button.



Enable/Disable Dynamic DNS

Dynamic DNS Status : Enable Disable

Apply

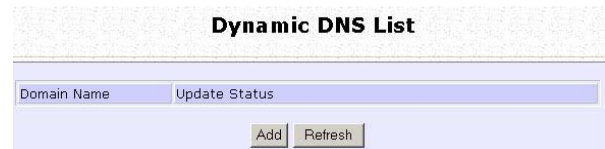
To manage Dynamic DNS List

Step 1:

Select **Dynamic DNS Setup** from the **Home User Features** command menu.

Step 2:

If you have created a list earlier, click on the **Refresh** button to update the list.



The screenshot shows a web interface titled "Dynamic DNS List". It features a table with two columns: "Domain Name" and "Update Status". Below the table, there are two buttons: "Add" and "Refresh".

Step 3:

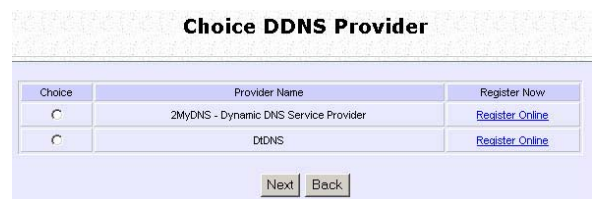
To add a new Dynamic DNS, click on the Add button.

The **Choice DDNS Provider** page appears.

There are two default providers that you can use.

The parameters are explained below:

- **Choice:**
Indicates your preferred DDNS provider.
- **Provider Name:**
Name of your preferred DDNS provider.
- **Register Now:**
Allows you to go to the website of your preferred DDNS provider where you can register your account.



The screenshot shows a web interface titled "Choice DDNS Provider". It contains a table with three columns: "Choice", "Provider Name", and "Register Now". There are two rows of providers listed. Below the table, there are two buttons: "Next" and "Back".

Choice	Provider Name	Register Now
<input type="radio"/>	2MyDNS - Dynamic DNS Service Provider	Register Online
<input type="radio"/>	DIDNS	Register Online

2 DDNS providers are predefined for you. You need to be connected to the Internet to register your DDNS account.

Select **2MyDNS – Dynamic DNS Service Provider** as DDNS Service Provider:

Step 1:
Under the **Choice** column in the **Choice DDNS Provider** list, check the radio button next to the **2MyDNS – DNS Service Provider** entry.

Click on the **Next** button.

Step 2:
Enter your **Domain Name**.

Step 3:
The **Auto Detect** checkbox is selected by default.
The **WAN IP** field is empty by default.
These default settings should be used if dynamic WAN IP connection is used.

If your ISP connection uses dynamic WAN IP:
Select the **Auto Detect** checkbox to let the DDNS server learn your current WAN IP address.
Enter your DDNS account **Username** and **Password**.

If your ISP connection uses a fixed WAN IP:
Enter the IP address in the **WAN IP** field.
Deselect the **Auto Detect** checkbox.
The access point will update the DDNS server with the specified WAN IP.

Step 4: Optional
Your hostname will be allowed multiple identities if wildcard is enabled.
For example, if you register: **mydomain.2mydns.net**, users looking for www.mydomain.2mydns.net or ftp.mydomain.2mydns.net can still reach your hostname.

Choice	Provider Name	Register Now
<input checked="" type="radio"/>	2MyDNS - Dynamic DNS Service Provider	Register Online
<input type="radio"/>	DDNS	Register Online

Next Back

Provider : 2MyDNS - Dynamic DNS Service Provider

Domain Name : [] 2mydns.net

WAN IP : [] Auto Detect

Username : []

Password : []

Wildcard : YES NO

Mail Exchanger : []

Backup Mail Exchanger : YES NO

Add Reset Back

Provider : 2MyDNS - Dynamic DNS Service Provider

Domain Name : [] 2mydns.net

WAN IP : []

Username : []

Password : []

Wildcard : YES NO

Mail Exchanger : []

Backup Mail Exchanger : YES NO

Add Reset Back

Step 5: Optional
In the Mail Exchanger field, enter the Static WAN IP address of the mail server configured to handle email for your domain.

Select **Backup Mail Exchanger** to enable this service.

Step 6:
Click on the Add button.

The new domain is added to the Dynamic DNS list table. It will appear as a hyperlink that you can click to go back to the Dynamic DNS Edit page.

Step 7:
From the Dynamic DNS Edit page you can update or reset the parameters, or delete the domain name.

Domain Name	Update Status
test.2mydns.net	

Provider : 2MyDNS - Dynamic DNS Service Provider
Domain Name : test . 2mydns.net

WAN IP : Auto Detect

Username :

Password :

Wildcard : YES NO

Mail Exchanger :

Backup Mail Exchanger : YES NO

Select **DtDNS** as DDNS Service Provider:

Step 1:

Under the **Choice** column in the **Choice DDNS Provider** list, check the radio button next to the **DtDNS** entry.

Click on the **Next** button.

Step 2:

Enter your **Domain Name**.

Step 3:

The **Auto Detect** checkbox is selected by default.

The **WAN IP** field is empty by default.

These default settings should be used if dynamic WAN IP connection is used.

If your ISP connection uses dynamic WAN IP:

Select the **Auto Detect** checkbox to let the DtDNS server learn your current WAN IP address.

Enter your DtDNS account **Username** and **Password**.

If your ISP connection uses a fixed WAN IP:

Enter the IP address in the **WAN IP** field.

Deselect the **Auto Detect** checkbox.

The access point will update the DtDNS server with the specified WAN IP.

Step 4:

Then click on the **Add** button.

Step 5:

While the new domain name is being added to the list, the message 'Waiting in queue...' will be displayed under the **Update Status** column of the **Dynamic DNS List** table.

Choice	Provider Name	Register Now
<input type="radio"/>	2MyDNS - Dynamic DNS Service Provider	Register Online
<input checked="" type="radio"/>	DtDNS	Register Online

Provider : **DtDNS**

Domain Name : . 3d-game.com

WAN IP : Auto Detect

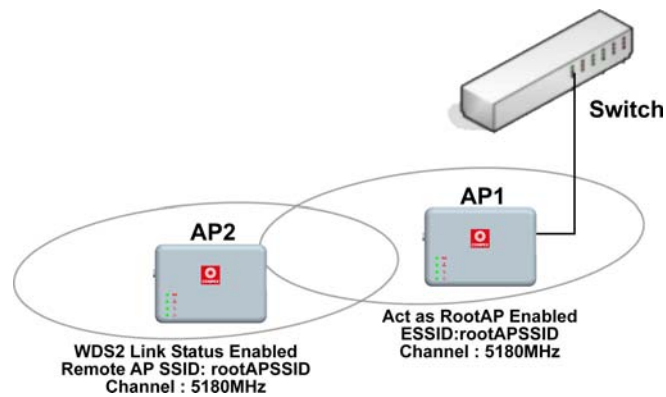
Password :

Domain Name	Update Status
esale.onlinesale.net	
cool.3d-game.com	Waiting in queue...

Use the Wireless Extended Features

Setup WDS2

WDS2 (Wireless Distributed System 2) links up access points to create a wider network in which mobile users can roam while still staying connected to available network resources. The wireless client and root access point has to be set up with the same channel frequency. This allows them to connect even when the link is lost, as the channel frequency setting is preserved.



In this example, there are 2 access points: Access Point 1 and Access Point 2, with Access Point 1 as the root access point.

Follow these steps to change the setup the root access point.

Setup access point 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Ensure that **The Current Mode** is set to **Access Point**.

To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

Select **Act as RootAP**.

Select the **Channel** common to both access point 1 and access point 2.

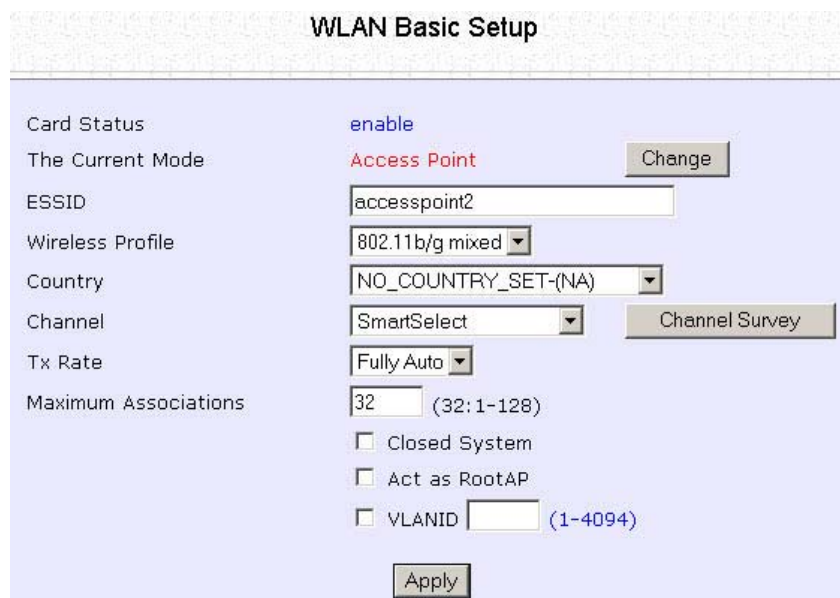
WLAN Basic Setup	
Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	<input type="text" value="rootAP"/>
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto
Maximum Associations	<input type="text" value="32"/> (32: 1-128)
	<input type="checkbox"/> Closed System
	<input checked="" type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/> (1-4094)
	<input type="button" value="Apply"/>

Follow these settings to setup access point 2.

Setup access point 2:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Select the **Channel** common to both access point 1 and access point 2.



The screenshot shows the 'WLAN Basic Setup' configuration page. The settings are as follows:

Parameter	Value	Buttons
Card Status	enable	
The Current Mode	Access Point	Change
ESSID	accesspoint2	
Wireless Profile	802.11b/g mixed	
Country	NO_COUNTRY_SET-(NA)	
Channel	SmartSelect	Channel Survey
Tx Rate	Fully Auto	
Maximum Associations	32 (32: 1-128)	
	<input type="checkbox"/> Closed System	
	<input type="checkbox"/> Act as RootAP	
	<input type="checkbox"/> VLANID [] (1-4094)	
	Apply	

Configure WDS2 link:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Advanced**.

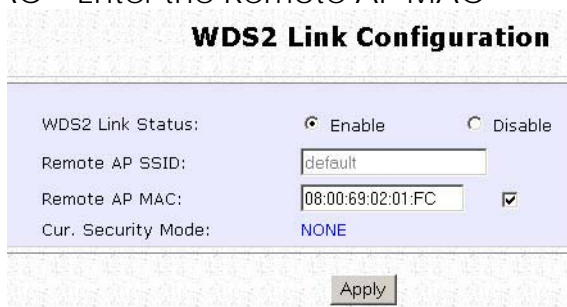


Under **Extended Features**, click on the **WDS2 Settings** button.

Set **WDS2 Link Status** to **Enable**.

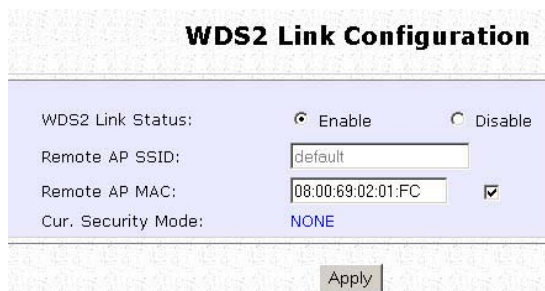
Options for configuring WDS2 link:

- By Remote AP MAC – Enter the Remote AP MAC

A screenshot of the "WDS2 Link Configuration" form. The form has a title bar "WDS2 Link Configuration". Below the title bar are four rows of settings: "WDS2 Link Status:" with radio buttons for "Enable" (selected) and "Disable"; "Remote AP SSID:" with a text box containing "default"; "Remote AP MAC:" with a text box containing "08:00:69:02:01:FC" and a checked checkbox; and "Cur. Security Mode:" with the value "NONE". At the bottom of the form is an "Apply" button.

OR

- By Remote AP SSID – Uncheck the Remote AP MAC checkbox and enter the Remote AP SSID.

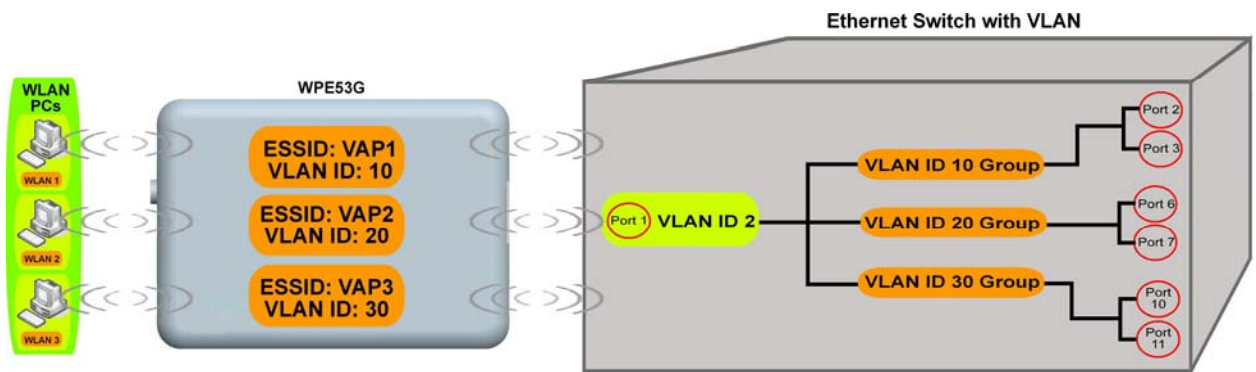
A screenshot of the "WDS2 Link Configuration" form, identical to the one above, but with the checkbox next to the "Remote AP MAC" field unchecked.

Click **Apply**.

Set Virtual AP (Multiple SSID)

Virtual AP implements mSSID (Multi-SSID) whereby a single wireless card can be setup with up to 16 virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.

Virtual AP delivers multiple services by VLAN segmentation: making the network think there are many SSIDs available and channeling each connection through different VLANs to the respective virtual network segments on the Ethernet network.



How it Works

When WLAN PC 1 connects to VAP 1 its packets are channeled to VLAN 10 group where only services connected to Port 2 and Port 3 are available to this wireless connection.

It is similar for WLAN PC 2 and WLAN PC 3. Although they connect to the same radio card as WLAN PC 1, WLAN PC 2 can only access the services available at Port 6 and Port 7 and WLAN PC 3 can only access the services available at Port 10 and Port 11.

For more information on Virtual AP (Multiple SSID) please refer to Appendix: Virtual AP (Multiple SSID) FAQ.

Follow these steps to setup Virtual AP.

Virtual AP

1

Click on **WLAN Setup** from the **CONFIGURATION** menu.
Select **Virtual AP**.

Virtual AP List

En	ESSID	BSSID	Statistics	Security	
<input checked="" type="checkbox"/>	Main	XX-XX-XX-XX-XX-XX	View	NONE	Delete
<input checked="" type="checkbox"/>	Sub	XX-XX-XX-XX-XX-XX	View	NONE	Delete

(All changes will take effect after reboot)

2

Virtual AP List page displays.

- Click Apply to register changes.
- Click Clear to clear Virtual AP List.
- Click Back to return to WLAN Basic Setup page.
- Select the Delete option beside any Virtual APs you wish to delete.

Click Add to goto add Virtual AP page.

Virtual AP

ESSID:

VLAN ID:

Closed System

RootAP

Security Mode:

3

1. Enter ESSID name.
2. Settings:
 - VLAN ID
 - Closed System
 - RootAP
3. Select Security Mode
4. Click Apply to make changes or click Back to return to Virtual AP List page.

Set Preferred APs

(Available in Client Mode)

When there is more than one AP with the same SSID, the Preferred APs function allows you define the MAC address of the APs in order of preference.

The MAC address at the top of the Preferred APs list has the highest connection preference, and the MAC address at the bottom has the lowest connection preference.

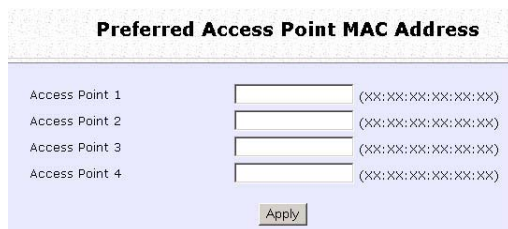
Follow these steps to specify your preferred APs.

Preferred APs

1

1. Click on [WLAN Setup](#) from the **CONFIGURATION** menu.

2. Select Preferred APs.



The screenshot shows a configuration page titled "Preferred Access Point MAC Address". It contains four rows, each labeled "Access Point 1" through "Access Point 4". Each row has a text input field followed by a placeholder "(XX:XX:XX:XX:XX:XX)". Below the input fields is an "Apply" button.

2

1. Enter the MAC addresses of the preferred APs.

2. Click Apply to effect the settings.

Get Long Distance Parameters

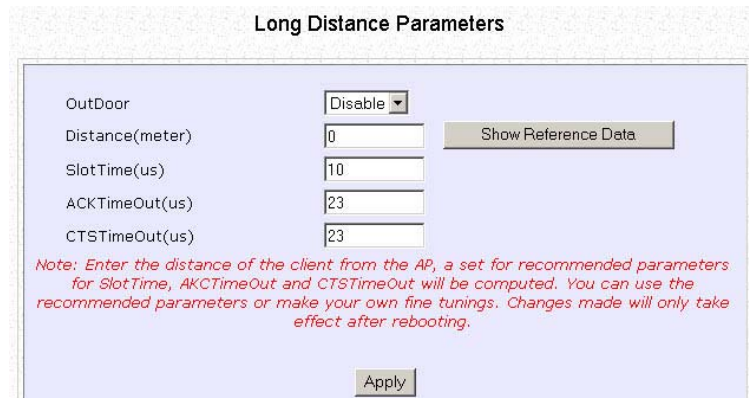
The access point can calculate and display suggested values for certain parameters to use to ensure that efficient wireless communication between physically distant access points.

Select **Advanced** from **WLAN Setup** under **Configuration**.

Click on the **Long Distance Parameters** button under the **Extended Features** section.



Select to **Enable** the **Outdoor** function.

A screenshot of the 'Long Distance Parameters' configuration page. The title 'Long Distance Parameters' is centered at the top. Below it is a form with the following fields:

- OutDoor: A dropdown menu with 'Disable' selected.
- Distance(meter): A text input field with '0' entered.
- SlotTime(us): A text input field with '10' entered.
- ACKTimeOut(us): A text input field with '23' entered.
- CTSTimeOut(us): A text input field with '23' entered.

To the right of the 'Distance(meter)' field is a button labeled 'Show Reference Data'. Below the form is a red note: *Note: Enter the distance of the client from the AP, a set for recommended parameters for SlotTime, AKCTimeOut and CTSTimeOut will be computed. You can use the recommended parameters or make your own fine tunings. Changes made will only take effect after rebooting.* At the bottom of the form is an 'Apply' button.

The access point can automatically calculate the values of the parameters to input based on the distance between your access point and the other wireless device. Enter the distance in meters and click on the **Show Reference Data** button.

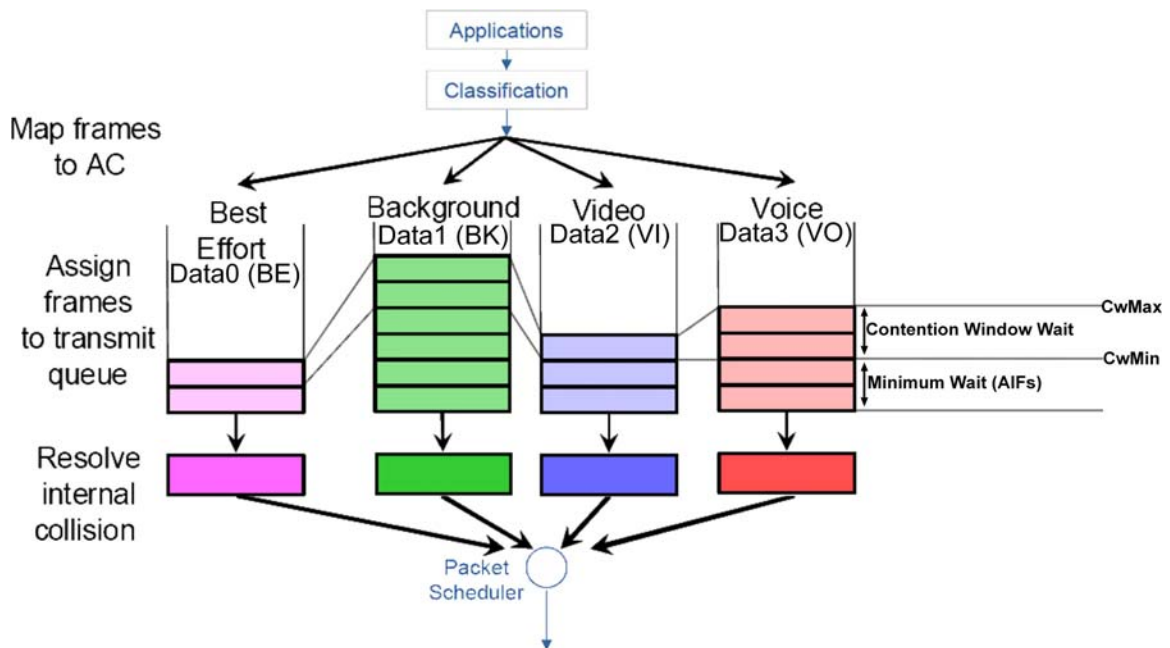


You can enter the parameters based on the recommended values in the pop-up window, click on the **Apply** button to update the changes.

Long Distance Parameters	Description
Outdoor	If set to Enable, the Outdoor parameters will be configured for outdoor communication over short or long distances as specified, it is disabled by default.
Distance	Determines the distance between your access point and the remote access point in meters.
Slot Time	The amount of time is divided and each unit of time is called one slot time.
ACK Timeout	Determines the timeout allowed for the sending client to receive the acknowledgment response from the receiving client. If no acknowledgment packet is received within this period, the sender will assume the receiver has not received the packet and will attempt to resend.
CTS Timeout	Clear-to-Send Timeout is the time the wireless sender will wait for a CTS packet signaling that the channel is idle and it can start data transmission. If no CTS packet is received within this period, the sender will assume the channel is busy and will wait before trying to send again.

Set Wireless Multimedia

Wireless Multimedia (WMM) is a QoS (Quality of Service) standard in IEEE802.11E that we have adopted to improve and support the user experience for multimedia, video, and voice applications by prioritizing data traffic. QoS can be realized through 4 different Access Categories (AC). Each AC type consists of an independent transmit queue, and a channel access function with its own parameters.



Follow these steps to change the setup Wireless Multimedia on your access point.

Step 1:

1. Click on **WLAN Setup** from the **CONFIGURATION** menu.
2. Select Advanced.

Step 2:

Click on the **WMM Settings** button.



Step 3:

Select to Enable **Wireless Multimedia (WMM)**

Enter the desired WMM parameters. Using the default parameters is recommended.

Click **Apply** to apply the WMM settings, click **Default** to reset all parameters to default, or click **Back** to discard any changes and return to WLAN Basic Setup page.

The image shows a screenshot of the 'WMM Setup' configuration page. It includes a title bar 'WMM Setup', a section for 'Wireless Multimedia (WMM)' with 'Enable' selected, and two tables for 'AP WMM Parameters' and 'Station WMM Parameters'. At the bottom are 'Apply', 'Default', and 'Back' buttons, and a note: '(All changes will take effect after reboot)'.

WMM Setup					
Wireless Multimedia (WMM) <input checked="" type="radio"/> Enable <input type="radio"/> Disable					
AP WMM Parameters:					
	AIFs	cwMin	cwMax	TxOp limit	NoAck
Data0 (BE)	3	15	63	0	<input type="checkbox"/>
Data1 (BK)	7	15	1023	0	<input type="checkbox"/>
Data2 (VI)	1	7	15	3008	<input type="checkbox"/>
Data3 (VO)	1	3	7	1504	<input type="checkbox"/>
Station WMM Parameters:					
	AIFs	cwMin	cwMax	TxOp limit	ACM
Data0 (BE)	3	15	1023	0	<input type="checkbox"/>
Data1 (BK)	7	15	1023	0	<input type="checkbox"/>
Data2 (VI)	2	7	15	3008	<input type="checkbox"/>
Data3 (VO)	2	3	7	1504	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Default"/> <input type="button" value="Back"/>					
<i>(All changes will take effect after reboot)</i>					

WMM Parameters (for advanced users)	
AIFs (Arbitrary Inter-Frame Space)	Arbitrary Inter-Frame Space is the minimum wait time interval between the wireless medium becoming idle and the start of transmission of a frame over the network.
Cwmin (Contention Window Minimum)	Contention Window Minimum is the minimum random wait time drawn from this interval or window for the backoff mechanism on the network.
CwMax (Contention Window Maximum)	Contention Window Maximum is the maximum random wait time drawn from this interval or window for the backoff mechanism on the network.
TxOp limit (Transmit Opportunity Limit)	Transmit Opportunity limit specifies the minimum duration that an end-user device can transmit data traffic after obtaining a transmit opportunity. TxOp limit can be used to give data traffic longer and shorter access.
NoAck (No Acknowledgement)	No Acknowledgement provides control of the reliability of traffic flow. Usually an acknowledge packet is returned for every packet received, increasing traffic load and decreasing performance. Enabling No Acknowledgement cancels the acknowledgement. This is useful for data traffic where speed of transmission is important.
ACM (Admission Control Mandatory)	Admission Control Mandatory enables WMM on the radio interface. When ACM is enabled, associated clients must complete the WMM admission control procedure before access.
BE (Best Effort)	Parameters for Data0 Best Effort. Best Effort data traffic has no prioritization and applications equally share available bandwidth.
BK (Background)	Parameters for Data1 Background. Background data traffic is de-prioritized and is mostly for backup applications, or background transfers like backup applications or background transfers like bulk copies that do not impact ongoing traffic like Internet downloads.
VI (Video)	Parameters for video data traffic.
VO (Voice)	Parameters for voice data traffic.

Setup Point-to-Point & Point-to-MultiPoint Connection

You can implement Point-to-Point connection by simply setting one access point as RootAP in Access Point mode and setting the other access points to Transparent Client mode.

You can set a root access point and a transparent client to allow point-to-point communication between different buildings and enable you to bridge wireless clients that are kilometres apart while unifying the networks. Or you can set a root access point and multiple transparent clients to allow point-to-multiple-point communication between the access point located at a facility and several other access points installed in any direction from that facility.

Follow these steps to setup RootAP

RootAP Step 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Ensure that **The Current Mode** is set to **Access Point**.

To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

WLAN Basic Setup	
Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	rootAP
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto
Maximum Associations	32 (32:1-128)
	<input type="checkbox"/> Closed System
	<input type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/> (1-4094)
	<input type="button" value="Apply"/>

RootAP Step 2:

Select **Act as RootAP**, click on the **Apply** button and reboot your device to let your changes take effect.

The screenshot shows the 'WLAN Basic Setup' configuration page. The settings are as follows:

Field	Value
Card Status	enable
The Current Mode	Access Point (Change button)
ESSID	rootAP
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect (Channel Survey button)
Tx Rate	Fully Auto
Maximum Associations	32 (32: 1-128)
Closed System	<input type="checkbox"/>
Act as RootAP	<input checked="" type="checkbox"/>
VLANID	<input type="checkbox"/> (1-4094)

An 'Apply' button is located at the bottom of the configuration area.

Follow these steps to setup Transparent Client/s.

Transparent Client Step 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Ensure that **The Current Mode** is set to **Transparent Client**.

To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

WLAN Basic Setup	
Card Status	enable
The Current Mode	Transparent Client <input type="button" value="Change"/>
ESSID	client <input type="button" value="Site Survey"/>
Remote AP MAC	00:00:00:00:00:00 <input type="checkbox"/>
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto
<input type="button" value="Apply"/>	

Transparent Client Step 2:

Select the **Remote AP MAC** checkbox.

Enter the **Remote AP MAC**.

WLAN Basic Setup	
Card Status	enable
The Current Mode	Transparent Client <input type="button" value="Change"/>
ESSID	client <input type="button" value="Site Survey"/>
Remote AP MAC	09:00:2B:23:00:00 <input checked="" type="checkbox"/>
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto
<input type="button" value="Apply"/>	

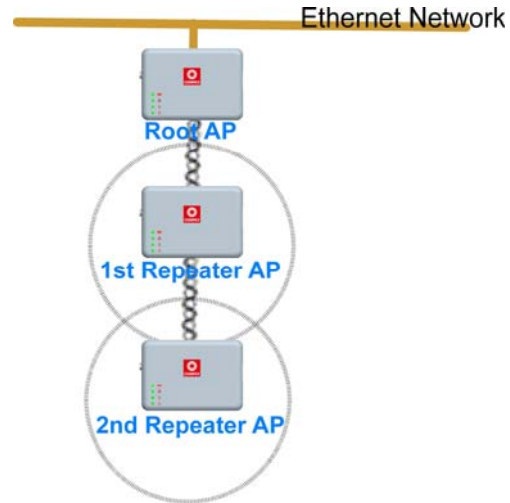
Note:

When using **Remote AP MAC**, the **ESSID** name must also match the AP's ESSID name, especially when Closed System is enabled on the AP.

Repeat Transparent Client step to add more points to the Point-to-MultiPoint connection.

Setup Repeater

A Repeater AP can connect to an AP only if the option **Act as RootAP** is set or checked in the AP setup.



Example: Network diagram with 2 repeater hops.



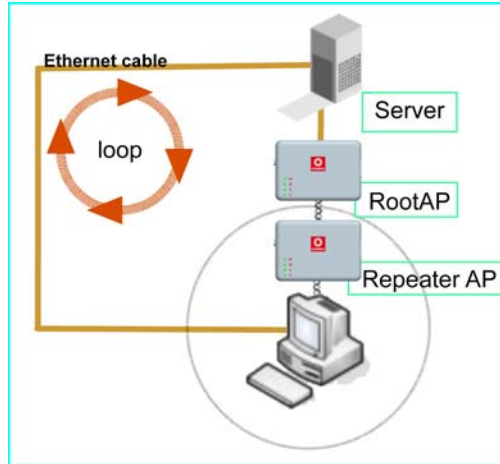
NOTE

As bandwidth degrades with every repeater hop it is recommended that a limit of **4 hops** is not exceeded.



NOTE

DO NOT physically connect your PC to the server via Ethernet cable in addition to the wireless connection, as doing so will create a loop that is not prevented by wireless loop preventing feature.



Follow these settings to setup the root AP.

Root AP Settings:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Ensure that **The Current Mode** is set to **Access Point**.

To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

Select **Act as RootAP**.

WLAN Basic Setup	
Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	root
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto
Maximum Associations	32 (32: 1-128)
	<input type="checkbox"/> Closed System
	<input checked="" type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID (1-4094)
	<input type="button" value="Apply"/>

Click **Apply**.

Follow these settings to setup the repeater.

Repeater Settings:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Ensure that **The Current Mode** is set to **Repeater**.

To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.



The screenshot shows the 'Repeater Basic Setup' configuration page. The settings are as follows:

Setting	Value	Action
Card Status	enable	
The Current Mode	Repeater	Change
ESSID	repeater	
Remote ESSID	default	Site Survey
Remote BSSID	00:00:00:00:00:00	<input type="checkbox"/>
Wireless Profile	802.11b/g mixed	
Country	NO_COUNTRY_SET-(NA)	
Tx Rate	Fully Auto	
	<input type="checkbox"/> Closed System	
		Apply

Options for defining the root AP:

- Accept the default **Remote ESSID** (root AP's SSID)

ESSID	<input type="text" value="repeater"/>
Remote ESSID	<input type="text" value="default"/>

OR

- Enter the **Remote ESSID**.

Remote ESSID	<input type="text" value="root"/>
Remote BSSID	<input type="text" value="00:00:00:00:00:00"/> <input type="checkbox"/>

OR

- Check and enter the **Remote BSSID** (root AP's MAC address)

Remote ESSID	<input type="text" value="default"/>
Remote BSSID	<input type="text" value="00:80:48:3d:0f:81"/> <input checked="" type="checkbox"/>

Click **Apply**.

Secure your Wireless LAN

Step 1:

Select **Security** from **WLAN Setup** under the **CONFIGURATION** menu.

Step 2:

Make a selection from the **Security Mode** drop-down list. The **Security Mode** is set to **NONE** by default.

Click on the **Apply** button.

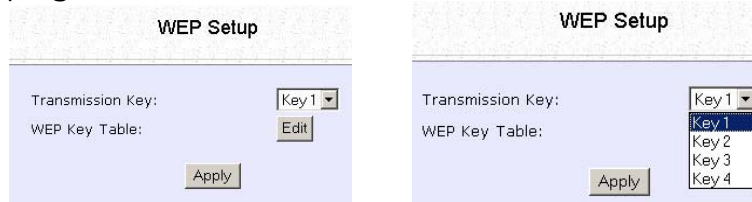


NOTE

All nodes in your network must share the same wireless settings in order to communicate.

Setup WEP

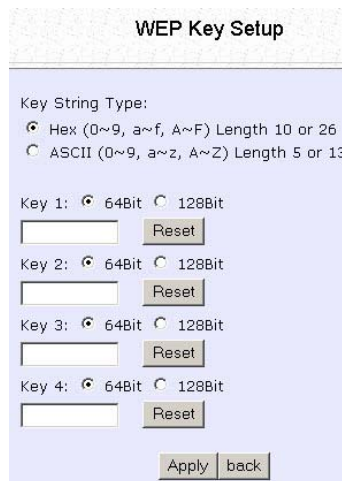
At the **WEP Setup** page,



Step 1:

Select the **Transmission Key** from the pull down menu:

- **Key 1**
- **Key 2**
- **Key 3**
- **Key 4**



Step 2:

Specify the **key entry type**, by selecting either:

- **Use Hexadecimal:**
- **Use ASCII**

The access point lets you define up to four different transmission keys. It defines a set of shared keys for network security. You must enter at least one WEP key to enable security using a shared key.

Step 3:

Select the **length** of each encryption key:

- **64-bit WEP**

10 hexadecimal or 5 ASCII Text

- **128-bit WEP**

26 hexadecimal or 13 ASCII Text

To clear the values that you have entered in the field, click on the **Reset** button.

Click on the **Apply** button and reboot your access point.

Setup WPA-Personal

(Available in Access Point, Repeater and Gateway Modes)

Follow these steps if you have activated the **WPA-Personal**, **WPA2-Personal** or **WPA-Personal-AUTO** security modes.

At the **WPA1/2-PSK Setup** page,

The screenshot shows the 'WPA1/2-PSK Setup' configuration page. It includes the following fields and options:

- Key String Type:** Two radio buttons are present: 'Hexadecimal(64 hex digits)' (unselected) and 'Passphrase(8~63 ascii characters)' (selected).
- WPA-PSK:** A text input field containing a masked key string (represented by asterisks).
- Cipher Type:** A dropdown menu currently set to 'AUTO', with a list of options including 'TKIP', 'AES', and 'AUTO'.
- GTK Update(seconds):** A text input field with a value of '60' and a range indicator '(60~9999)' to its right.
- Apply:** A button located at the bottom right of the form.

Step 1:

Specify the **key entry type**, by selecting either:

- **Passphrase (Alphanumeric characters)**
- **Hexadecimal**

Step 2:

Fill in the pre-shared network key:

If you are using the **Passphrase** format, your entry can consist of a minimum of 8 alphanumeric characters or a maximum of 63 alphanumeric characters.

Otherwise, when using the **Hexadecimal** format, your entry MUST consist of 64 hexadecimal characters.

Step 3:

For WPA-Personal

Set the **Cipher Type** to **TKIP**.

WPA replaces WEP with a strong encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC).

For WPA2-Personal

Set the **Cipher Type** to **AES**.

Advanced Encryption Standard (AES) is a stronger symmetric 128-bit block data encryption technique. AES is a requirement of WPA2 under the IEEE 802.11i standard.

For WPA-Personal-AUTO

Set the **Cipher Type** to **Auto** to allow the access point to automatically detect the cipher type to use.

Step 4:

Enter the **GTK (Group Transient Key) Updates**.

This is the length of time after which the access point will automatically generate a new shared key to secure multicast/broadcast traffic among all stations that are communicating with it. By default, the value is 600 seconds.

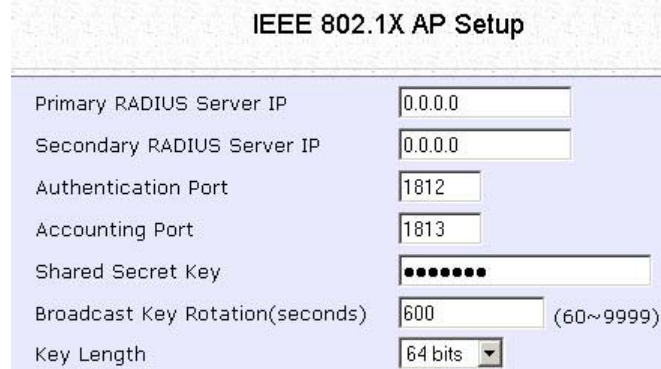
Step 5:

Click the **Apply** button and reboot your system, after which your settings will become effective.

Setup 802.1x/RADIUS for Access Point

(Available in Access Point, Repeater and Gateway Modes)

At the IEEE 802.1x AP Setup page,



The screenshot shows the 'IEEE 802.1X AP Setup' configuration page. It contains the following fields and values:

Field	Value
Primary RADIUS Server IP	0.0.0.0
Secondary RADIUS Server IP	0.0.0.0
Authentication Port	1812
Accounting Port	1813
Shared Secret Key	••••••••
Broadcast Key Rotation(seconds)	600 (60~9999)
Key Length	64 bits

Step 1:

Key in the IP address of the **Primary RADIUS Server** in your WLAN. You can optionally add in the IP address of a **Secondary RADIUS Server**, if any.

The RADIUS authentication server MUST be in the same subnet as the access point.

Step 2:

By default, the value for **Authentication Port** number is **1812**. You can leave this value as it is. This value must be set to be the same as the one in the RADIUS server.

Step 3:

By default, the value for **Accounting Port** number is **1813**. You can leave this value as it is. This value must be set to be the same as the one in the RADIUS server.

Step 4:

Enter the **Shared Secret Key** in the field provided.

Step 5:

By default, the **Broadcast Key Rotation** is set as **600** seconds. You may leave this value as its default setting.

Step 6:

Select the **length** of each encryption key:

- **64-bit**

10 hexadecimal or 5 ASCII Text

- **128-bit**

26 hexadecimal or 13 ASCII Text

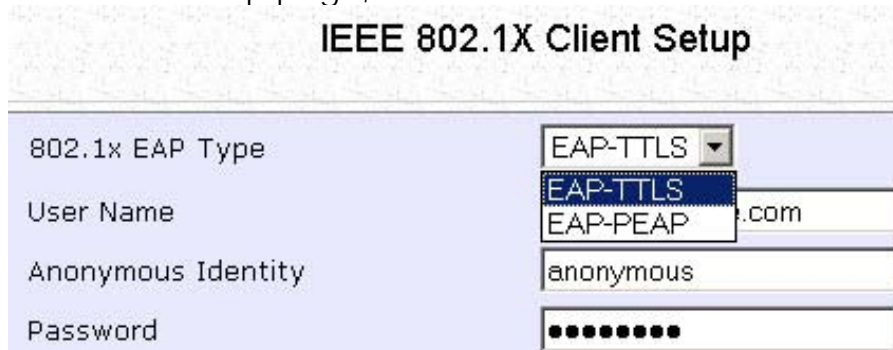
Step 7:

Click the **Apply** button and reboot your system, after which your settings will become effective.

Setup 802.1x/RADIUS for Client

(Available in Client, Transparent Client, Wireless Routing Client and Wireless Adapter Modes)

At the IEEE 802.1x Client Setup page,



The screenshot shows the 'IEEE 802.1X Client Setup' page. The '802.1x EAP Type' dropdown menu is open, showing 'EAP-TTLS' as the selected option. Other options visible are 'EAP-PEAP' and 'EAP-PEAP'. The 'User Name' field contains '.com', 'Anonymous Identity' is 'anonymous', and 'Password' is masked with dots.

Step 1:

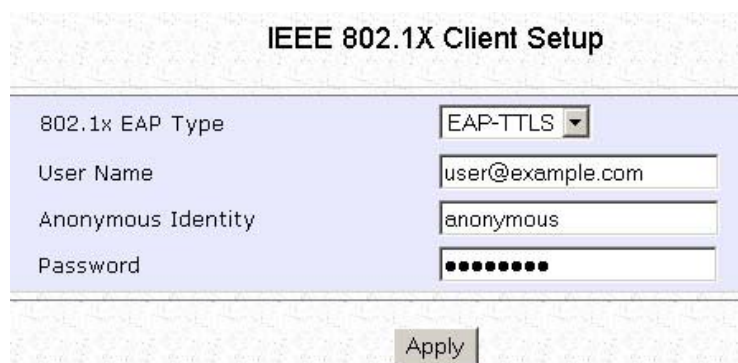
Select whether to use **EAP-TTLS** or **EAP-PEAP** 802.1x EAP Type.

Step 2:

Both **EAP-TTLS** (Extensible Authentication Protocol - Tunneled Transport Layer Security) and **EAP-PEAP** (Protected Extensible Authentication Protocol) support identity hiding. In the WLAN, the access point generates an identity request. To preserve anonymity, the client responds with only enough information to allow the RADIUS server to process the request.

If using **EAP-TTLS** 802.1x EAP Type:

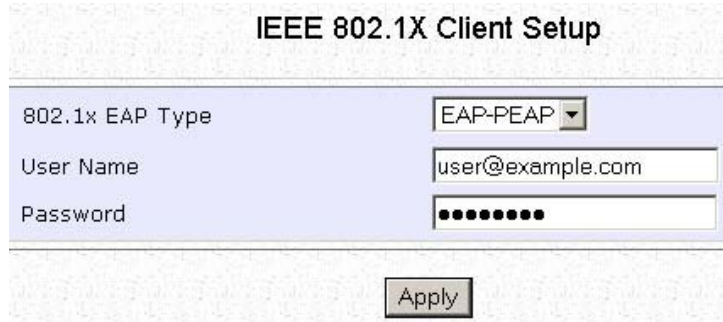
- Enter the **User Name**.
- Enter the **Anonymous Identity** attribute for EAP-TTLS.
- Enter the **Password**.



The screenshot shows the 'IEEE 802.1X Client Setup' page with the following fields filled out: '802.1x EAP Type' is 'EAP-TTLS', 'User Name' is 'user@example.com', 'Anonymous Identity' is 'anonymous', and 'Password' is masked with dots. An 'Apply' button is visible at the bottom.

If using **EAP-PEAP 802.1x EAP Type**:

- Enter the **User Name**.
- Enter the **Password**.



The screenshot shows a web form titled "IEEE 802.1X Client Setup". It contains three input fields: a dropdown menu for "802.1x EAP Type" set to "EAP-PEAP", a text box for "User Name" containing "user@example.com", and a password field for "Password" with ten dots. An "Apply" button is located at the bottom center of the form.

Step 3:

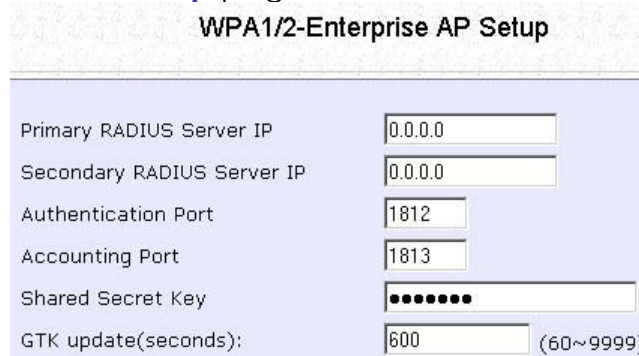
Click the **Apply** button and reboot your system, after which your settings will become effective.

Setup WPA Enterprise for Access Point

(Available in Access Point, Repeater and Gateway Modes)

Follow these steps if you have selected the **WPA1-Enterprise**, **WPA2-Enterprise**, or **WPA-Enterprise-AUTO** security modes.

At the **WPA1/2-Enterprise AP Setup** page,



WPA1/2-Enterprise AP Setup	
Primary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Secondary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Authentication Port	<input type="text" value="1812"/>
Accounting Port	<input type="text" value="1813"/>
Shared Secret Key	<input type="password" value="••••••••"/>
GTK update(seconds):	<input type="text" value="600"/> (60~9999)

Step 1:

Key in the IP address of the **Primary RADIUS Server** in your WLAN.

You can optionally add in the IP address of a **Secondary RADIUS Server**, if any. The RADIUS authentication server MUST be in the same subnet as the access point.

Step 2:

By default, the value for **Authentication Port** number is **1812**. You can either leave this value as it is or key in a different Authentication Port but it MUST match the corresponding port of the RADIUS server.

Step 3:

By default, the value for **Accounting Port** is **1813**. You can leave this value as it is. This value must be set to be the same as the one in the RADIUS server.

Step 4:

Enter the **Shared Secret Key** used to validate client-server RADIUS communications.

Step 5:

Enter the **GTK (Group Transient Key) Updates**.

This is the length of time after which the access point will automatically generate a new shared key to secure multicast/broadcast traffic among all stations that are communicating with it. By default, the value is 600 seconds.

Step 6:

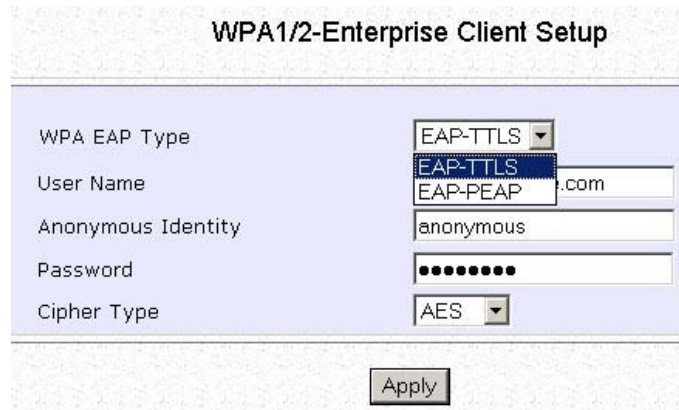
Click the **Apply** button and reboot your system, after which your settings will become effective.

Setup WPA Enterprise for Client

(Available in Client, Transparent Client, Wireless Routing Client and Wireless Adapter Modes)

Follow these steps if you have selected the **WPA1-Enterprise**, **WPA2-Enterprise**, or **WPA-Enterprise-AUTO** security modes.

At the **WPA1/2-Enterprise Client Setup** page,



The screenshot shows a web-based configuration interface titled "WPA1/2-Enterprise Client Setup". The interface has a light blue background and contains the following fields:

- WPA EAP Type:** A dropdown menu with "EAP-TTLS" selected. A tooltip is visible showing "EAP-TTLS" and "EAP-PEAP".
- User Name:** A text input field containing ".com".
- Anonymous Identity:** A text input field containing "anonymous".
- Password:** A text input field with ten black dots representing a masked password.
- Cipher Type:** A dropdown menu with "AES" selected.

At the bottom center of the form is an "Apply" button.

Step 1:

Select whether to use **EAP-TTLS** or **EAP-PEAP** **WPA EAP Type**.

Step 2:

Both **EAP-TTLS** (Extensible Authentication Protocol - Tunneled Transport Layer Security) and **EAP-PEAP** (Protected Extensible Authentication Protocol) support identity hiding. In the WLAN, the access point generates an identity request. To preserve anonymity, the client responds with only enough information to allow the RADIUS server to process the request.

If using **EAP-TTLS** **WPA EAP Type**:

- Enter the **User Name**.
- Enter the **Anonymous Identity** attribute for EAP-TTLS.
- Enter the **Password**.
- Enter the **Cipher Type**.

For WPA-Enterprise

Set the **Cipher Type** to **TKIP**.

WPA replaces WEP with a strong encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC).

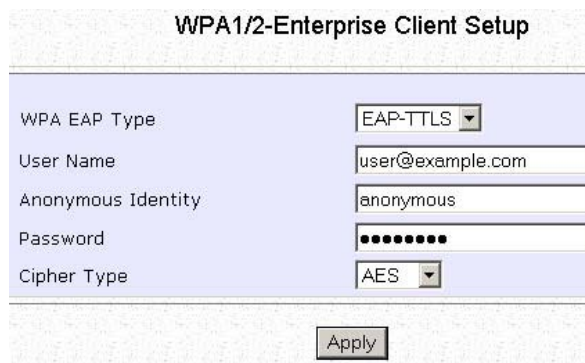
For WPA2- Enterprise

Set the **Cipher Type** to **AES**.

Advanced Encryption Standard (AES) is a symmetric 128-bit block data encryption technique. It is a requirement of WPA2 under the IEEE 802.11i standard.

For WPA- Enterprise -AUTO

Set the **Cipher Type** to **Auto** to allow the access point to automatically detect the cipher type to use.



The screenshot shows a configuration window titled "WPA1/2-Enterprise Client Setup". It contains the following fields and values:

Field	Value
WPA EAP Type	EAP-TTLS
User Name	user@example.com
Anonymous Identity	anonymous
Password	••••••••
Cipher Type	AES

An "Apply" button is located at the bottom center of the window.

If using **EAP-PEAP WPA EAP Type**:

- Enter the **User Name**.
- Enter the **Anonymous Identity** attribute for EAP-TTLS.
- Enter the **Password**.
- Enter the **Cipher Type**.

For WPA-Enterprise

Set the **Cipher Type** to **TKIP**.

WPA replaces WEP with a strong encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC).

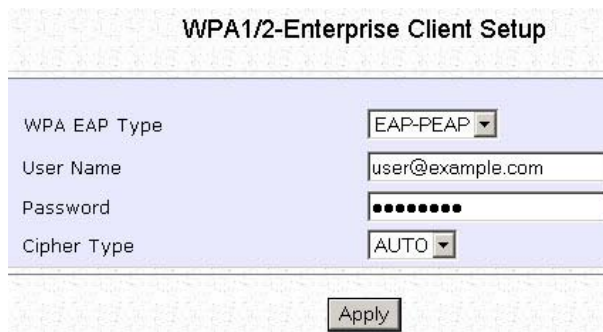
For WPA2- Enterprise

Set the **Cipher Type** to **AES**.

Advanced Encryption Standard (AES) is a symmetric 128-bit block data encryption technique. It is a requirement of WPA2 under the IEEE 802.11i standard.

For WPA- Enterprise -AUTO

Set the **Cipher Type** to **Auto** to allow the access point to automatically detect the cipher type to use.



The screenshot shows a configuration window titled "WPA1/2-Enterprise Client Setup". It contains four fields: "WPA EAP Type" with a dropdown menu set to "EAP-PEAP", "User Name" with a text box containing "user@example.com", "Password" with a text box containing ten dots, and "Cipher Type" with a dropdown menu set to "AUTO". An "Apply" button is located at the bottom center of the window.

Step 3:

Click the **Apply** button and reboot your system, after which your settings will become effective.

Configure the Security Features

Use Packet Filtering

Packet filtering selectively allows /disallows applications from Internet connection.

Configure Packet Filtering

(Available in Wireless Routing Client and Gateway modes)

Step 1:

Select **Packet Filtering** from the **Security Configuration** command menu.



Packet Filter Configuration


Packet Filter Type : Disabled

Step 2:

Select the **Packet Filter Type** by clicking on the **Change** button.

Step 3:

Select from three choices: **Disabled**, **Sent**, **Discarded**, and then click on the **Apply** button. The default is **Disabled**, which allows all packets to be sent.

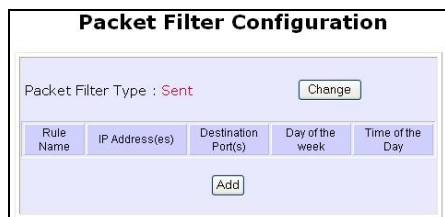


Select Packet Filtering Type

Disabled All IP packets will be sent.

Sent All IP packets will be sent except for those matching one or more of the rules.

Discarded All IP packets will be discarded except for those matching one or more of the rules.



Packet Filter Configuration

Packet Filter Type : Sent

Rule Name	IP Address(es)	Destination Port(s)	Day of the week	Time of the Day



Add a new Packet Filter 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 : Mon

To : Fri

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

From : (hh:mm)

To : (hh:mm)

Step 4:

Click on the **Add** button and you will be able to define the details of your **Packet Filter Rule** from the screen on the right.

4a). Enter **Rule Name** for this new packet filtering rule. For example, *BlockCS*

4b). From the **IP Address** drop down list, select whether to apply the rule to:



Rule Name :

- A **Range** of IP addresses
In this case, you will have to define **(From)** which IP address **(To)** which IP address, your range extends.

IP Address : **Range** ▼
From : 192.168.168. 25
To : 192.168.168. 75

- A **Single** IP address
Here, you need only specify the source IP address in the **(From)** field.

IP Address : **Single** ▼
From : 192.168.168. 25
To : 192.168.168.

- **Any** IP address
You may here, leave both, the **(From)** as well as the **(To)** fields, blank. Here, the rule will apply to all IP addresses.

IP Address : **Any** ▼
From : 192.168.168.
To : 192.168.168.

4c). At the **Destination Port** drop down list, select either:

- A **Range** of TCP ports
In this case, you will have to define **(From)** which port **(To)** which port, your rule applies.

Destination Port : **Range** ▼
From : 21
To : 81

- A **Single** TCP port
Here, you need only specify the source port in the **(From)** field.

Destination Port : **Single** ▼
From : 25
To :

- **Any** IP port
You may here, leave both, the **(From)** as well as the **(To)** fields, blank. Here, the rule will apply to all ports.

Destination Port : **Any** ▼
From :
To :

4d). From the **Day of the Week** drop down list, select whether the rule should apply to:

- A **Range** of days
Here, you will have to select **(From)** which day **(To)** which day

Day of the Week : **Range** ▼
From : **Wed** ▼
To : **Fri** ▼

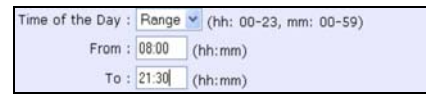
- **Any** day
In this case, you may skip both the **(From)** as well as the **(To)** drop down fields.

Day of the Week : **Any** ▼
From : **Sun** ▼
To : **Sun** ▼

4e). At the **Time of the Day** drop down list, you may also choose to apply the rule to:

- A **Range** of time

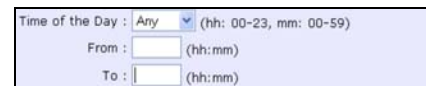
In which case, you have to specify the time in the format **HH:MM**, where **HH** may take any value from 00 to 23 and **MM**, any value from 00 to 59.



Time of the Day : Range (hh: 00-23, mm: 00-59)
From : 08:00 (hh:mm)
To : 21:30 (hh:mm)

- **Any** time

Here, you may leave both **(From)** and **(To)** fields blank.



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

Step 5:

Click on the **Apply** button to make the new rule effective.

The **Filtering Configuration** table will then be updated.



Add a new Packet Filter rule

Rule Name : BlockCS
IP Address : Any
From : 192.168.168.
To : 192.168.168.
Destination Port : Single
From : 27015
To : 27015
Day of the Week : Range
From : Mon
To : Fri
Time of the Day : Range (hh: 00-23, mm: 00-59)
From : 07:00 (hh:mm)
To : 18:00 (hh:mm)
Add Cancel Help

Step 6:

In this example, we would block an application called CS from all PCs (any IP address within the network) from Monday to Friday 7am to 6pm, and this application is using the port number 27015.

Therefore, for a rule we name BlockCS, and add the entries depicted on the left. Clicking on the **Add** button will effect your packet filter rule.

Use URL Filtering

URL Filtering allows you to block objectionable websites from your LAN users.

Configure URL Filtering

(Available in Wireless Routing Client and Gateway modes)

Step 1:

Select **URL Filtering** from the **Security Configuration** command menu.



Step 2:

To select the **URL Filter Type**, click the **Change** button.

Step 3:

Select to **Block** or **Allow**, and then click on the **Apply** button. The default is **Disabled**, which allows all websites to be accessed.



Then click the **Add** button.



Step 4:

For the **Host Name** field, input the web site address that you wish to block. Then click the **Add** button to complete your setup.

Configure the Firewall

Configure SPI Firewall

(Available in Wireless Routing Client and Gateway modes)

Stateful Packet Inspection (SPI) thwarts common hacker attacks like IP Spoofing, Port Scanning, Ping of Death, and SynFlood by comparing certain key parts of the packet to a database of trusted information before allowing it through.



NOTE

Firewall security rules should be planned carefully as incorrect configuration may cause improper network function.

Select **Firewall Configuration** from the **Security Configuration** command menu.

Enable the firewall. You can choose among the **Default Low**, **Default Medium** or **Default High** security options for convenient setup.

Then you may choose the type of network activity information you wish to log for reference. Data activity arising from different types of protocol can be recorded.

Firewall Configuration

Warning: Incorrect configuration may cause undesirable behavior.

Firewall Status: Enable Disable

Allow user visit LAN from WAN port

Log Information

Accepted: TCP Packets UDP Packets
 ICMP Packets IGMP Packets

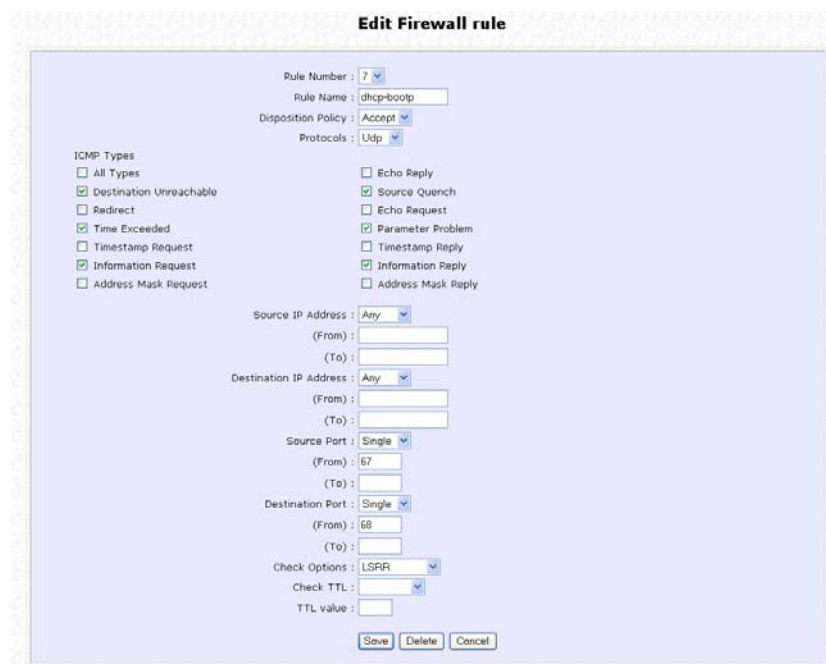
Denied: TCP Packets UDP Packets
 ICMP Packets IGMP Packets

No.	Active	Name	Disposition Policy	Protocol	Source Address(es)	Destination Address(es)	Source Ports	Destination Ports
0	<input type="checkbox"/>	ICMP-DENY	Deny	ICMP	Any	Any	Any	Any
1	<input type="checkbox"/>	TCP-DENY	Deny	TCP	Any	Any	Any	Any
2	<input checked="" type="checkbox"/>	icmp	Accept	ICMP	Any	Any	Any	Any
3	<input checked="" type="checkbox"/>	udp	Accept	UDP	Any	Any	53	Any
4	<input checked="" type="checkbox"/>	ftp(20-21)	Accept	TCP	Any	Any	Any	20-21
5	<input checked="" type="checkbox"/>	ftp(80)	Accept	TCP	Any	Any	Any	80
6	<input checked="" type="checkbox"/>	ssh	Accept	UDP	Any	Any	1545	Any
7	<input checked="" type="checkbox"/>	ftp-broto	Accept	UDP	Any	Any	87	88

Add Apply

Default Low Default Medium Default High

You may add more firewall rules for specific security purposes. Click on the **Add** radio button at the screen shown above, followed by the **Edit** button.



Rule Name : Enter a unique name to identify this firewall rule.

Disposition Policy : This parameter determines whether the packets obeying the rule should be accepted or denied by the firewall. Choose between Accept and Deny.

Protocols : Users are allowed to select the type of data packet from: TCP, UDP, ICMP, IGMP or ALL.

Note: If users select either ICMP or IGMP, they are required to make further selection in the ICMP Types or IGMP Types respectively.

ICMP Types : This IP protocol is used to report errors in IP packet routing. ICMP serves as a form of flow control, although ICMP messages are neither guaranteed to be received or transmitted.

ICMP Packet Type	Description
Echo request	Determines whether an IP node (a host or a router) is available on the network.
Echo reply	Replies to an ICMP echo request.

Destination unreachable	Informs the host that a datagram cannot be delivered.
Source quench	Informs the host to lower the rate at which it sends datagrams because of congestion.
Redirect	Informs the host of a preferred route.
Time exceeded	Indicates that the Time-to-Live (TTL) of an IP datagram has expired.
Parameter Problem	Informs that host that there is a problem in one of the ICMP parameters.
Timestamp Request	Information that is from the ICMP data packet.
Information Request	Information that is from the ICMP data packet.
Information Reply	Information that is from the ICMP data packet.

IGMP Types : This IP protocol 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.

Host Membership Report	Information that is from the IGMP data packet.
Host Membership Query	Information that is from the IGMP data packet.
Leave Host Message	Information that is from the ICMP data packet.

Source IP : This parameter allows you to specify workstation(s) generating the data packets. Users can either set a single IP address or set a range of IP addresses.

Destination IP : This parameter lets you specify the set of workstations that receive the data packets. Users can either set a single IP address or set a range of IP addresses.

Source Port : You can control requests for using a specific application by entering its port number here. Users can either set a single port number or a range of port numbers.

Destination Port : This parameter determines the application from the specified destination port. Users can either set a single port number or a range of port numbers.

Check Options : This parameter refers to the options in the packet header. The available selection options are abbreviated as follows:

SEC – Security
LSRR – Loose Source Routing
Timestamp – Timestamp
RR – Record Route
SID – Stream Identifier
SSRR – Strict Source Routing
RA – Router Alert

Check TTL : This parameter would let you screen packets according to their Time-To-Live (TTL) value available options are:

1. Equal
2. Less than
3. Greater than
4. Not equal

Use the Firewall Log

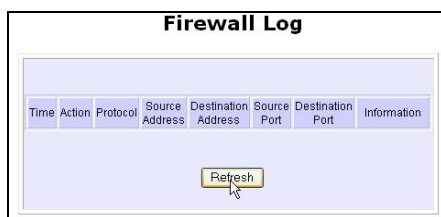
The Firewall Log captures and stores network traffic information such as the type of data traffic, the time, the source and destination address / port, as well as the action taken by the firewall.

View Firewall Logs

(Available in Wireless Routing Client and Gateway modes)

Step 1:

Select **Firewall Log** from the **SECURITY CONFIGURATION** command menu.



Step 2:

Click on the **Refresh** button to see the information captured in the log:

- **Time** at which the packet was detected by the firewall.
- **Action**, which states whether the packet was accepted or denied.
- **Protocol** type of the packet.
- **Source Address** from which the packet originated
- **Destination Address** to which the packet was intended.
- **Source Port** from which the packet was initiated.
- **Destination Port** to which the packet was meant for.
- Any **Information**.

Administer the System

Use the System Tools

Use the Ping Utility

(Available in Wireless Routing Client and Gateway modes.)

You can check whether the access point can communicate (ping) with another network host with the Ping Utility.

Step 1:

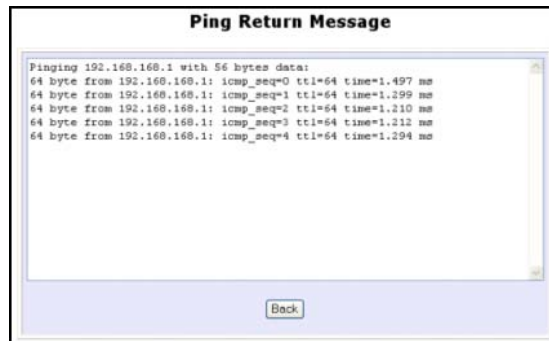
Select [Ping Utility](#) under the [SYSTEM TOOLS](#) command menu.



Step 2:

Enter the IP address of the target host to ping.

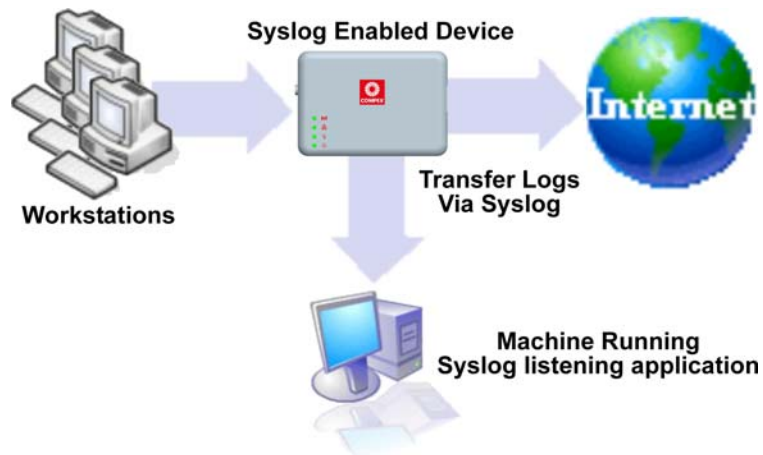
Click the [Start](#) button.



The Ping messages are displayed.

Use Syslog

Syslog forwards system log messages in a network to a machine running a Syslog listening application. It is used to help in managing the computer system and increase security on the network. Freeware supporting Syslog is widely available for download from the Internet.



This section shows how to:

- Setup Syslog.
- View logged information.

The System Log Setup page allows the user to:

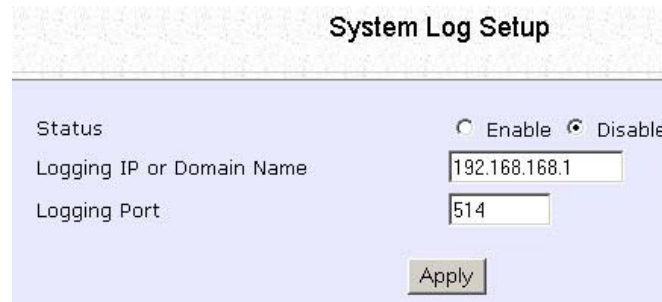
- **Enable** or **Disable** system logging.
- Set the **Remote IP Address or Domain Name** and **Remote Port** for the router to send the system log messages to.

Follow these steps to setup Syslog:

Step 1:

Click on **Syslog** from the **SYSTEM TOOLS** menu.

Step 2:



The screenshot shows a window titled "System Log Setup" with a light blue background. It contains the following fields and controls:

- Status:** Two radio buttons are present: "Enable" (which is unselected) and "Disable" (which is selected).
- Logging IP or Domain Name:** A text input field containing the value "192.168.168.1".
- Logging Port:** A text input field containing the value "514".
- Apply:** A button located at the bottom right of the form.

Select to **Enable** Syslog.

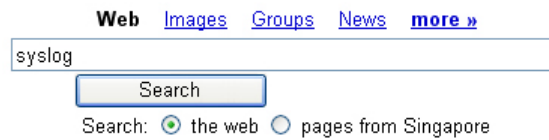
Enter the **Logging IP or Domain Name**

Enter the **Logging Port**

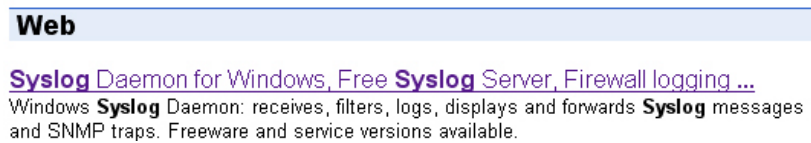
Click **Apply** to make the changes.

Follow these sample steps to view logged information:

Step 1:
Search for a Syslog listening application.



Step 2:
Select a Syslog listening application.



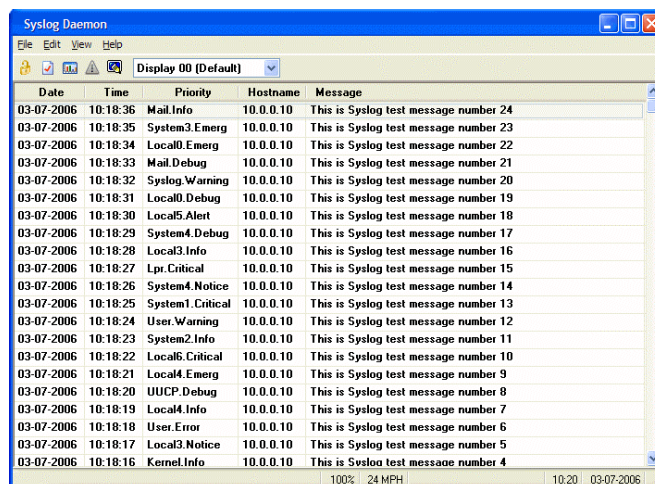
Step 3:
Download Syslog listening application.



Step 4:
Install Syslog listening application.



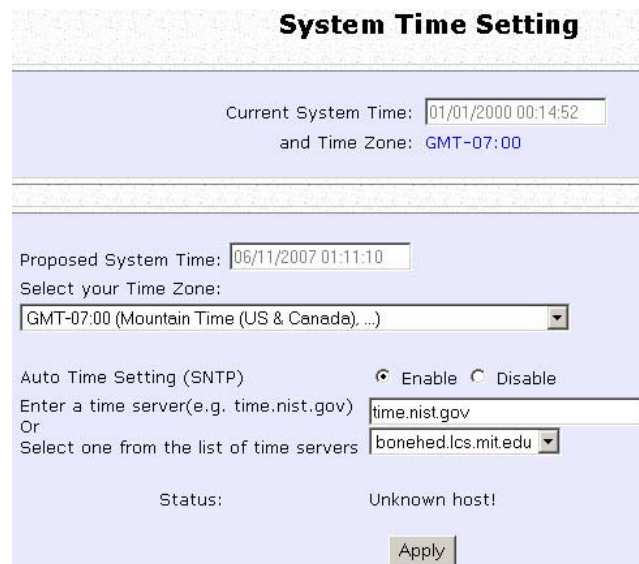
Step 5:
View logged information on Syslog listening application.



Setup System Clock

Step 1:

Select **System Clock Setup** from the **SYSTEM TOOLS** menu.



The screenshot shows a web interface titled "System Time Setting". At the top, it displays "Current System Time: 01/01/2000 00:14:52" and "and Time Zone: GMT-07:00". Below this, there is a section for "Proposed System Time: 06/11/2007 01:11:10" and "Select your Time Zone:" with a dropdown menu currently set to "GMT-07:00 (Mountain Time (US & Canada), ...)". Underneath, there are radio buttons for "Auto Time Setting (SNTP)" with "Enable" selected and "Disable" unselected. There are two input fields for time servers: "Enter a time server(e.g. time.nist.gov)" with "time.nist.gov" entered, and "Or Select one from the list of time servers" with a dropdown menu showing "bonehed.lcs.mit.edu". At the bottom, the status is "Unknown host!" and there is an "Apply" button.

Step 2:

Select the appropriate time zone from the **Select to Change the Time Zone for the Router Location** drop-down list.

Step 3:

Enable the Auto Time Setting (SNTP) radio button. **SNTP** stands for Simple Network Time Protocol and is used to synchronise computer clocks.

Step 4:

Fill in the **Time Servers** field and click on the **Apply** button to effect the changes.

Upgrade the Firmware with uConfig

You can check the types and version of your firmware by clicking on **About System** from the **HELP** menu.

To begin with, ensure that you have the updated firmware available.

Step 1:

Select **Firmware Upgrade** from the **SYSTEM TOOLS** menu.



Step 2:

Click on the **Browse** button to locate the file.

Step 3:

Click on the **Upgrade** button.

Follow the instructions given during the upgrading process.



Step 4:

You need to reboot the system after the firmware upgrade.



NOTE

The firmware upgrade process must NOT be interrupted; otherwise the device might become unusable.

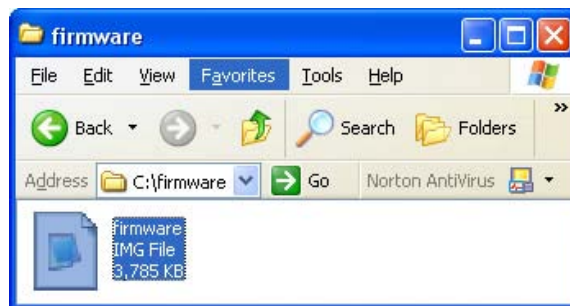
Upgrade the Firmware with Command Line Interface

You can check the types and version of your firmware by clicking on **About System** from the **HELP** menu in UConfig.

Follow these steps to upgrade firmware from Command Line Interface (CLI).

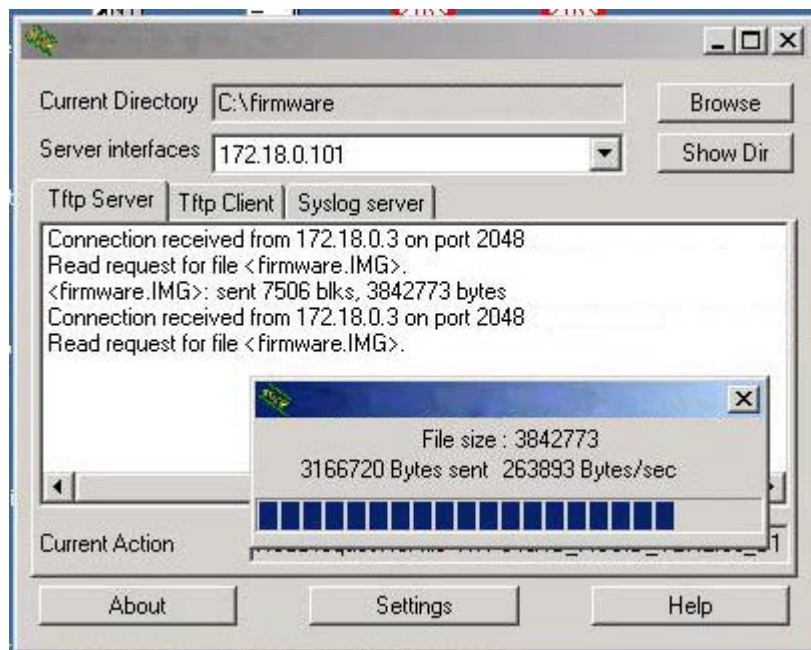
Step 1:

Ensure that you have the updated firmware available.



Step 2:

On the PC connected to the AP, run a TFTP server and setup to point to the same firmware image filename.

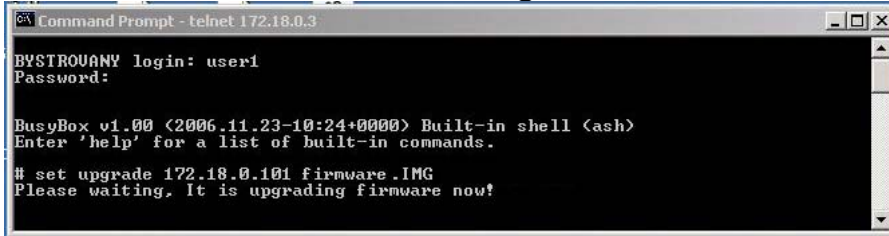


Sample Screenshot

Step 3:

In the Command Line Interface, enter the command with the IP address of the AP and the filename of the firmware image as the parameters:

Set upgrade <IP address of AP> <firmware image filename>



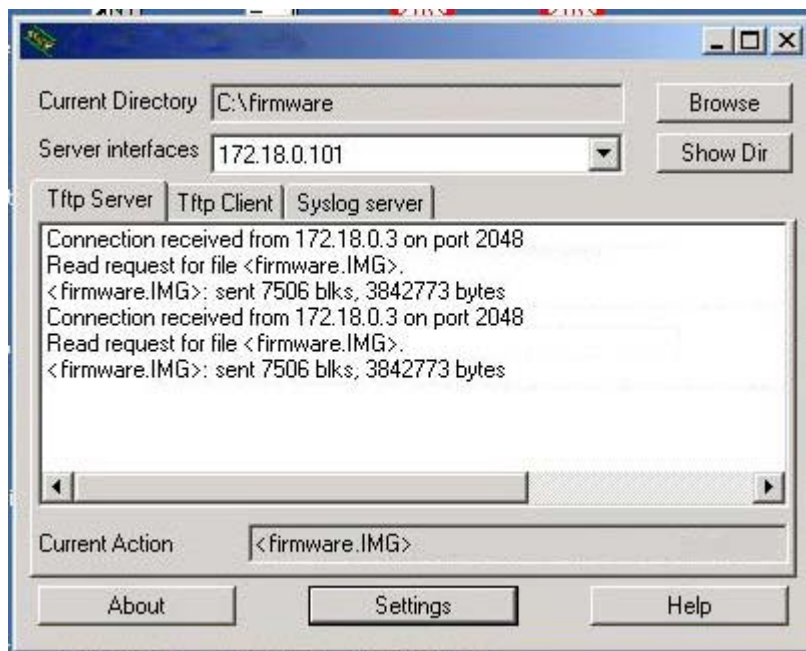
```
Command Prompt - telnet 172.18.0.3
BYSTROUANY login: user1
Password:

BusyBox v1.00 (2006.11.23-10:24+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

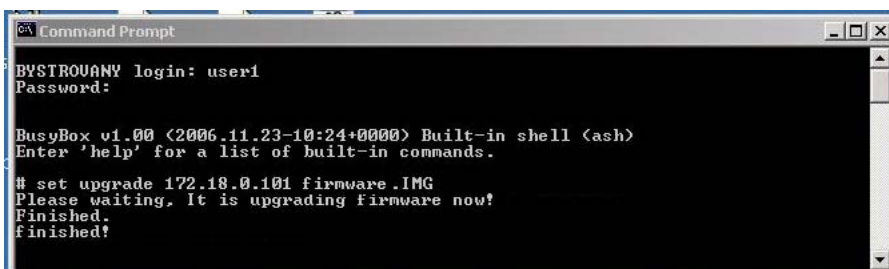
# set upgrade 172.18.0.101 firmware.IMG
Please waiting, It is upgrading firmware now!
```

Step 4:

These screens display when upgrade is done.



Sample Screenshot



```
Command Prompt
BYSTROUANY login: user1
Password:

BusyBox v1.00 (2006.11.23-10:24+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# set upgrade 172.18.0.101 firmware.IMG
Please waiting, It is upgrading firmware now!
Finished.
finished!
```



NOTE

The firmware upgrade process must NOT be interrupted; otherwise the device might become unusable.

Perform Firmware Recovery

If the system fails to launch properly, the access point will automatically switch to loader mode and the diagnostic LED will remain lighted. The firmware should then be reloaded.

Access Point State	Diagnostic LED (Y) State
Corrupted firmware – access point automatically switches to loader mode	Blinks very fast
Recovery in progress	ON
Successful recovery	Blinks very slowly

Before starting, check the status of the diagnostic LED to confirm if firmware failure has occurred.

Step 1:

Stop power supply and disconnect the access point from the network.

Step 2:

Connect the LAN port of the access point to the LAN port of your computer with an MDI cable.

Step 3:

Power on the access point, and start up your computer. You are recommended to set your computer's IP address to 192.168.168.100 and its network mask to 255.255.255.0.

It is recommended that your computer IP address is set to 192.168.168.100 and the network mask is set to 255.255.255.0

Step 4:

Insert the Product CD into the CD drive of your computer.

Step 5:

From the **Start** menu, click **Run** and type **cmd**. When the command prompt window appears, type in the following command:

X:\recovery\TFTP -i 192.168.168.1 PUT image_name.IMG, where **X** refers to your CD drive and **image_name.IMG** refers to the firmware filename found in the Recovery folder of the Product CD.

Step 6:

If you have downloaded a newer firmware and have saved it in your local hard disk as: **C:\accesspoint\accesspointxxx.IMG**, then replace the command with this new path and firmware name. For example:

C:\accesspoint\TFTP -i 192.168.168.1 PUT accesspointxxx.img

The recovery process takes place.

You can monitor the progress of the recovery process with the diagnostic LED.

When firmware restoration is complete, reboot the access point and it will be ready to operate.

Backup or Reset the Settings

You may choose to save the current configuration profile, create a backup of it on your hard disk, restore an earlier saved profile, or to reset the access point back to its default settings.

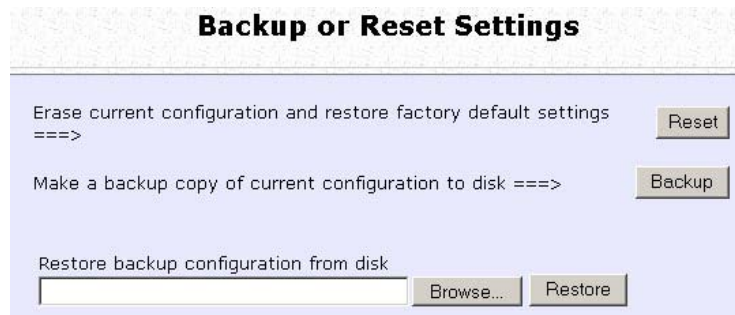
Reset your settings

Step 1:

Select **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

Step 2:

To discard configurations made and restore the access point to its initial factory settings, click on the **Reset** button.



Step 3:

The system will prompt you to reboot your device, click on the **Reboot** button.

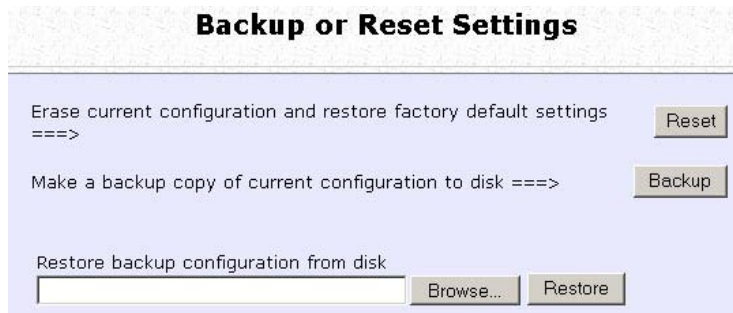
Backup your Settings

Step 1:

Select **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

Step 2:

To back up the current settings of your access point onto your hard disk drive, click on the **Backup** button.



Step 3:

Save your configuration file to your local disk.



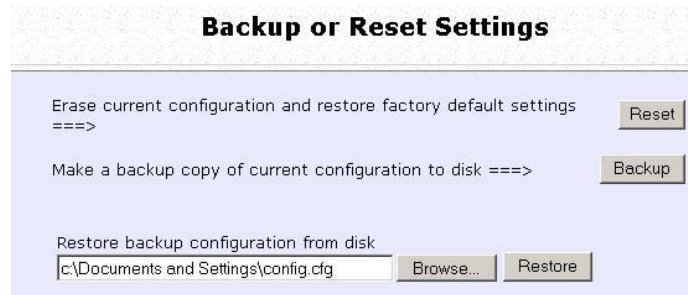
Restore your Settings

Step 1:

Select **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

Step 2:

To restore previously saved settings, click on the **Browse...** button and select the folder where you saved your configuration file.



Click on the **Restore** button and the system will prompt you to reboot your device.

Step 2:

Reboot the System

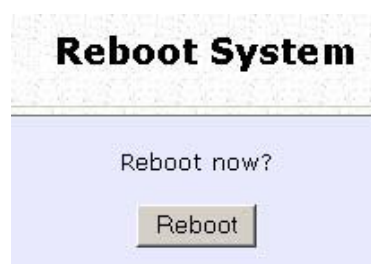
Most of the changes you make to the system settings require a system reboot before the new parameters can take effect.

Step 1:

Select **Reboot System** from the **SYSTEM TOOLS** menu.

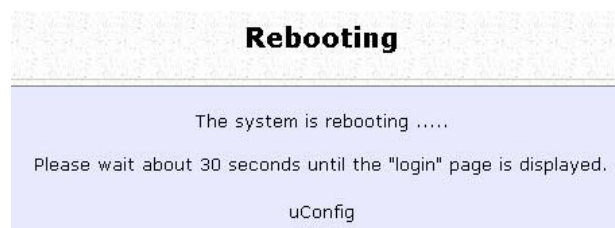
Step 2:

Click on the **Reboot** button.



Step 3:

Wait for the system to reboot and the login page will be displayed.



Change the Password

It is recommended that the login password is changed from the factory default password.

Step 1:

Select **Change Password** from the **SYSTEM TOOLS** menu.

Step 2:

Key in the **Current Password**. The password is case-sensitive and defaulted to *password*

Enter the **New Password** field and then **Confirm Password**.

Step 3:

Click on the **Apply** button to update the changes.



The screenshot shows a web form titled "Change Password". It contains three input fields for "Current Password", "New Password", and "Confirm Password", each with four dots indicating masked text. Below the fields is an "Apply" button.

Change Password	
Current Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
<input type="button" value="Apply"/>	

To Logout

Step 1:

Select **Logout** from the **SYSTEM TOOLS** menu.

Step 2:

Click the **LOGIN!** button to access the access point configuration interface again.



Use the HELP menu

View About System

System Information displays system configuration information that may be required by support technicians for troubleshooting.

Select **About System** from the **HELP** menu.

The **System Information** page displays information about the access point configuration settings.

System Information	
Device:	
System Up Time :	0 Days 00:01:32
BIOS/Loader Version :	2.41 (build 0516)
Firmware Version :	2.01 (build 20-April-2007)
NetWork Mode :	Inherent Bridge
Wireless:	
Hardware Address :	00-80-48-ff-00-2c
WLAN name (ESSID):	compex-wpe53g
Operating frequency :	2427MHz
Operating Channel :	4
Security Mode :	None
Management Port:	
Hardware Address :	00-80-48-ff-00-2b
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Disabled

Get Technical Support

This page displays the contact information of technical support centres around the world.

If further information unavailable in the manual or data sheet is required, please contact a Technical Support Centre by mail, email, fax or telephone.

Click on **Get Technical Support** from the **HELP** menu.

Support Information

To register your product, obtain product information, documentation and updates, go to:
<http://www.cpx.com>
<http://www.complex.com.sg>

Regional Technical Support Centers

U.S.A., Canada, Latin America and South America :

Complex Inc.
840 Columbia Street, Suite B, Brea, CA92821,USA
Tel : (714) 482-0333
Fax : (714) 482-0332
800 Line: (800) 279-8891
Email: support@cpx.com

Asia, Australia, New Zealand, Middle East and the rest of the world :

Complex Systems Pte. Ltd.
135, Joo Seng Road, #08-01,
PM Industrial Building
Singapore 368363
HotLine : (65) 6-286-1805
Fax : (65) 6-283-8337

Appendix: Use the Command Line Interface

Get Operation List

SYNTAX	DESCRIPTION
Get tasks	Display all active process/tasks.
Get sysinfo	Display system information.
Get aplist	Display list of access points discovered.
Get athstats	Display wireless driver information.
Get brinfo	Display bridge and interfaces information.
Get brmacshow	Display bridge learned MAC address list.
Get bssinfo.	Display current radio information.
Get channel	Display current wireless channel number.
Get chanlist	Display current domain wireless channels.
Get ieee80211stats	Display ieee80211 protocol statistics.
Get routeshow	Display the routing table information.
Get stalist	Display a list of currently associated stations.
Get linkinfo	Display client link information (Client mode only)
Get macstats	Display a list of currently learnt wireless device MAC addresses.
Get opmode	Display current wireless operation mode.
Get wmode	Display wireless mode

Set Operation List

SYNTAX	DESCRIPTION
Set factorydefault	Set factorydefault – restore configuration to factory default.
Restart	Do a warm reboot.

Save Configuration

SYNTAX	DESCRIPTION
Commit	Save current configuration to flash. Most commands require rebooting to take effect after saving.

Long Range

Check for recommended values from long distance option setup page.

SYNTAX	DESCRIPTION
Set outdoor <enable/disable>	Enable outdoor for long-range connection.
Set distance <value>	Set the connection distant (value in decimal)
Set acktimeout <value>	Set the ACK timeout (value in decimal)
Set cttimeout <value>	Set the CTS timeout (value in decimal)
Set slottimeout <value>	Set the Slot timeout (value in decimal)

TX Power

SYNTAX	DESCRIPTION
Set txpower <string>	(Default full) auto, 1, 2, 3, 4, ..., 17, full, min

TX Rate

SYNTAX	DESCRIPTION
Set txrate <string>	Values are: (default auto) (802.11a)-- 6, 9, 12, 18, 24, 36, 48, 54, auto (Version AG) (802.11b/g mixed)-- 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, auto (802.11b-only)-- 1, 2, 5.5, 11, auto

Wireless Mode

SYNTAX	DESCRIPTION
Set wirelessmode <string>	Supported strings are: auto, 11a, 11b, 11g, pureg, superg, supera
Set autochannelselect Enable/disable	Enable or disable smart channel select during power up.
Set radio_off_eth_down enable/disable	Enable or disable auto turn off radio when Ethernet port connection link is lost.

WEP Key

Must first set a key entry type, and then proceed to set the key index, size, and value.

SYNTAX	DESCRIPTION
Set key <keyindex> <keysize> <keyvalue>	Set keyentrymethod hex/ascii
Set key <keyindex> default	Set default key.

Add or Delete User

SYNTAX	DESCRIPTION
Set user < [-r] -w > <password> username	To add a user.
Set user -d username	To delete user.

Country Code

SYNTAX	DESCRIPTION
Set countrycode <iso.name>	List of countries: <pre>{0, "NA"}, {CTRY_ALBANIA, "AL"}, {CTRY_ALGERIA, "DZ"}, {CTRY_ARGENTINA, "AR"}, {CTRY_ARMENIA, "AM"}, {CTRY_AUSTRALIA, "AU"}, {CTRY_AUSTRIA, "AT"}, {CTRY_AZERBAIJAN, "AZ"}, {CTRY_BAHRAIN, "BH"}, {CTRY_BELARUS, "BY"}, {CTRY_BELGIUM, "BE"}, {CTRY_BELIZE, "BZ"}, {CTRY_BOLIVIA, "BO"}, {CTRY_BRAZIL, "BR"}, {CTRY_BRUNEI_DARUSSALAM, "BN"}, {CTRY_BULGARIA, "BG"}, {CTRY_CANADA, "CA"}, {CTRY_CHILE, "CL"}, {CTRY_CHINA, "CN"}, {CTRY_COLOMBIA, "CO"}, {CTRY_COSTA_RICA, "CR"}, {CTRY_CROATIA, "HR"}, {CTRY_CYPRUS, "CY"}, {CTRY_CZECH, "CZ"}, {CTRY_DENMARK, "DK"}, {CTRY_DOMINICAN_REPUBLIC, "DO"}, {CTRY_ECUADOR, "EC"}, {CTRY_EGYPT, "EG"}, {CTRY_EL_SALVADOR, "SV"}, {CTRY_ESTONIA, "EE"}, {CTRY_FINLAND, "FI"}, {CTRY_FRANCE, "FR"}, {CTRY_FRANCE2, "F2"}, {CTRY_GEORGIA, "GE"}, {CTRY_GERMANY, "DE"}, {CTRY_GREECE, "GR"}, {CTRY_GUATEMALA, "GT"}, {CTRY_HONDURAS, "HN"}, {CTRY_HONG_KONG, "HK"}, {CTRY_HUNGARY, "HU"}, {CTRY_ICELAND, "IS"}, {CTRY_INDIA, "IN"}, {CTRY_INDONESIA, "ID"}, {CTRY_IRAN, "IR"}, {CTRY_IRELAND, "IE"}, {CTRY_ISRAEL, "IL"},</pre>
Set countrycode <2 letter string>	

	<pre> {CTRY_ITALY, "IT"}, {CTRY_JAPAN, "JP"}, {CTRY_JAPAN1, "J1"}, {CTRY_JAPAN2, "J2"}, {CTRY_JAPAN3, "J3"}, {CTRY_JAPAN4, "J4"}, {CTRY_JAPAN5, "J5"}, {CTRY_JAPAN6, "J6"}, {CTRY_JORDAN, "JO"}, {CTRY_KAZAKHSTAN, "KZ"}, {CTRY_KOREA_NORTH, "KP"}, {CTRY_KOREA_ROC, "KR"}, {CTRY_KOREA_ROC2, "K2"}, {CTRY_KOREA_ROC3, "K3"}, {CTRY_KUWAIT, "KW"}, {CTRY_LATVIA, "LV"}, {CTRY_LEBANON, "LB"}, {CTRY_LIECHTENSTEIN, "LI"}, {CTRY_LITHUANIA, "LT"}, {CTRY_LUXEMBOURG, "LU"}, {CTRY_MACAU, "MO"}, {CTRY_MACEDONIA, "MK"}, {CTRY_MALAYSIA, "MY"}, {CTRY_MALTA, "MT"}, {CTRY_MEXICO, "MX"}, {CTRY_MONACO, "MC"}, {CTRY_MOROCCO, "MA"}, {CTRY_NETHERLANDS, "NL"}, {CTRY_NEW_ZEALAND, "NZ"}, {CTRY_NORWAY, "NO"}, {CTRY_OMAN, "OM"}, {CTRY_PAKISTAN, "PK"}, {CTRY_PANAMA, "PA"}, {CTRY_PERU, "PE"}, {CTRY_PHILIPPINES, "PH"}, {CTRY_POLAND, "PL"}, {CTRY_PORTUGAL, "PT"}, {CTRY_PUERTO_RICO, "PR"}, {CTRY_QATAR, "QA"}, {CTRY_ROMANIA, "RO"}, {CTRY_RUSSIA, "RU"}, {CTRY_SAUDI_ARABIA, "SA"}, {CTRY_SINGAPORE, "SG"}, {CTRY_SLOVAKIA, "SK"}, {CTRY_SLOVENIA, "SI"}, {CTRY_SOUTH_AFRICA, "ZA"}, {CTRY_SPAIN, "ES"}, {CTRY_SWEDEN, "SE"}, {CTRY_SWITZERLAND, "CH"}, {CTRY_SYRIA, "SY"}, {CTRY_TAIWAN, "TW"}, {CTRY_THAILAND, "TH"}, {CTRY_TRINIDAD_Y_TOBAGO, "TT"}, {CTRY_TUNISIA, "TN"}, {CTRY_TURKEY, "TR"}, {CTRY_UKRAINE, "UA"}, {CTRY_UAE, "AE"}, {CTRY_UNITED_KINGDOM, "GB"}, {CTRY_UNITED_STATES, "US"}, {CTRY_URUGUAY, "UY"}, {CTRY_UZBEKISTAN, "UZ"}, {CTRY_VENEZUELA, "VE"}, {CTRY_VIET_NAM, "VN"}, {CTRY_YEMEN, "YE"}, {CTRY_ZIMBABWE, "ZW"}, </pre>
--	--

Channel

SYNTAX	DESCRIPTION
Set channel <value>	(Value in decimal)

SSID

SYNTAX	DESCRIPTION
Set ssid <string>	(Not More than 32 characters)

Closed System

SYNTAX	DESCRIPTION
Set hidessid enable/disable	Enable or disable broadcasting of SSID.

Per Node

SYNTAX	DESCRIPTION
Set apbridge enable/disable	Enable or disable isolation of wireless client.

RTS, Fragment, and Beacon Interval

SYNTAX	DESCRIPTION
Set rts <value>	(Value in decimal, default 2312, range 1 to 2312)
Set fragment <value>	(Value in decimal, default 2346, range, 256 to 2346)
Set beaconintval <value>	(Value in decimal, default 1, range 1 to 1000)
Set dtim <value>	Data Beacon Rate (value in decimal, default 1, range 1 to 16384)

WLAN State

SYNTAX	DESCRIPTION
Get wlanstate	Display whether status of current wireless operation is Enabled or Disabled.
Set wlanstate enable/disable	Set to Disable to turn off wireless operation. Set to Enable to turn back on wireless operation. Note: When executing this command, please ensure that you are not connected on wireless with device or you will be disconnected from the device and network. The wireless operation can only be Enabled from the Ethernet port or UTP cable connection to device.

Reset Button

SYNTAX	DESCRIPTION
Get buttonpassreset	Display the status of Reset Button operation. If status is (Enabled), resetting of password by pressing Reset Button is allowed. If status is (Disabled), resetting of password by pressing Reset Button is not allowed.
Set buttonpassreset enable/disable	Set to Disable to prevent resetting of password by pressing Reset button. Set to Enable to allow resetting of password by pressing Reset button.

Upgrade Firmware

SYNTAX	DESCRIPTION
Set upgrade <IP address of AP> <firmware image filename>	
DESCRIPTION	To upgrade firmware in CLI enter this command with the IP address of AP and the firmware image filename.

Custom Configuration Update

SYNTAX	Cfgfile <operation type> <IP of PC running TFTP server> <filename>										
DESCRIPTION	<p>The cfgfile command is used for managing simple configuration changes to multiple access points. It is useful for when the user has many access points to configure and the configuration is mostly the same.</p> <p>For example if user needs to configure ten access points, and just change the IP address configuration:</p> <ol style="list-style-type: none"> 1. Configure the first access point with the common configuration for all the access points using web manager 2. Export the access point configuration file with cfgfile in Telnet. 3. Edit the IP addresses in the access point configuration files to customise them for the individual access points. 4. Import the edited access point configuration files to the respective access points with cfgfile in Telnet. <p>Requirement and Explanation:</p> <p>The cfgfile command uses the TFTP (Trivial File Transfer Protocol). This command transfers the access point configuration file to and from the access point. It has 4 operation types for these transfers – Backup, Restore, Export, and Import.</p> <p>Before executing the cfgfile command, there are some requirements that have to be met in order for the command to execute successfully. The TFTP server has to be running on the PC with the Telnet connection to the access point.</p> <p>Make a note of the directory where the access point configuration file is located in. This directory can be a folder on the hard drive of the PC with the Telnet connection. It can also be any storage device that is connected to this PC. The TFTP server has to be set up to point to this directory.</p> <p style="text-align: center;">This table explains the different Operation Types.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th colspan="2" style="text-align: center;">Operation Type</th> </tr> </thead> <tbody> <tr> <td style="width: 20%;">Backup</td> <td> <p>The Backup operation saves the configuration from the access point to the configuration file defined in <filename> and stored on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(Access Point → PC)</p> </td> </tr> <tr> <td>Restore</td> <td> <p>The Restore operation returns the access point back to the previous configuration according to the configuration file defined in <filename> on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(PC → Access Point)</p> </td> </tr> <tr> <td>Export</td> <td> <p>The Export operation extracts a portion of the access point configuration to a text file on the PC which can be edited to further customise it for each access point.</p> <p>This text file can then be imported into other access points with the Import cfgfile operation.</p> <p>(Access Point → PC)</p> </td> </tr> <tr> <td>Import</td> <td> <p>The Import Operation uploads the configuration to the access point.</p> <p>This configuration is the access point configuration which has been exported previously with the Export cfgfile operation and then further edited to customise for each access point.</p> <p>(PC → Access Point)</p> </td> </tr> </tbody> </table>	Operation Type		Backup	<p>The Backup operation saves the configuration from the access point to the configuration file defined in <filename> and stored on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(Access Point → PC)</p>	Restore	<p>The Restore operation returns the access point back to the previous configuration according to the configuration file defined in <filename> on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(PC → Access Point)</p>	Export	<p>The Export operation extracts a portion of the access point configuration to a text file on the PC which can be edited to further customise it for each access point.</p> <p>This text file can then be imported into other access points with the Import cfgfile operation.</p> <p>(Access Point → PC)</p>	Import	<p>The Import Operation uploads the configuration to the access point.</p> <p>This configuration is the access point configuration which has been exported previously with the Export cfgfile operation and then further edited to customise for each access point.</p> <p>(PC → Access Point)</p>
Operation Type											
Backup	<p>The Backup operation saves the configuration from the access point to the configuration file defined in <filename> and stored on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(Access Point → PC)</p>										
Restore	<p>The Restore operation returns the access point back to the previous configuration according to the configuration file defined in <filename> on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(PC → Access Point)</p>										
Export	<p>The Export operation extracts a portion of the access point configuration to a text file on the PC which can be edited to further customise it for each access point.</p> <p>This text file can then be imported into other access points with the Import cfgfile operation.</p> <p>(Access Point → PC)</p>										
Import	<p>The Import Operation uploads the configuration to the access point.</p> <p>This configuration is the access point configuration which has been exported previously with the Export cfgfile operation and then further edited to customise for each access point.</p> <p>(PC → Access Point)</p>										

Appendix: Virtual AP (Multi-SSID) FAQ

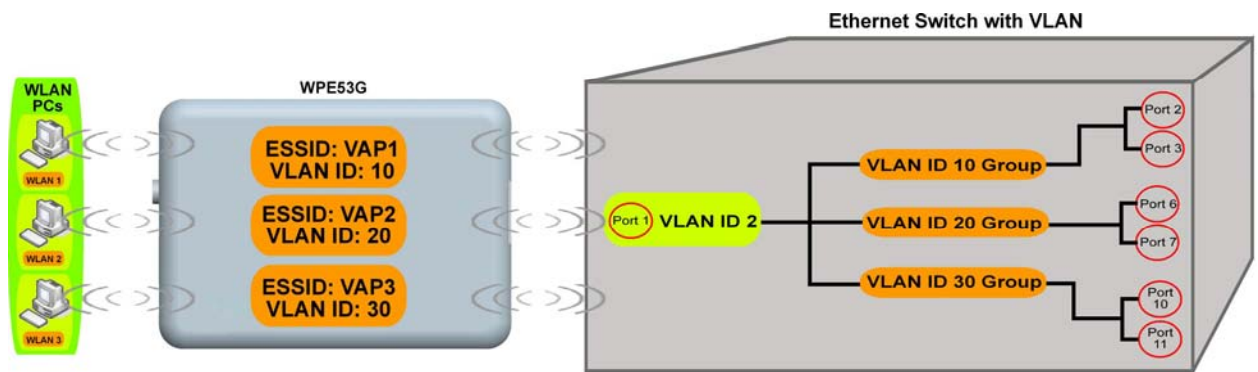
Q1) What is mSSID?

Multi-SSID (mSSID) as the name suggest, allows an access point (AP) with a single radio card to support more than one SSID.

Q2) What can you do with mSSID connection?

The application of mSSID is to provide better security with multiple network path connections from a single AP, to multiple VLAN network segments of the switch on the local area network.

A network setup application is illustrated below.



E.g.

Virtual AP with SSID: VAP1, VLAN ID: 10 and WPA-PSK wireless security enabled will be channeled to Port 2 and Port 3 where the internet-sharing router is connected.

Virtual AP with SSID: VPA2, VLAN ID: 20, WPA-EAP enabled, and connected to a radius server, will be channeled to Port 5 and Port 6, which are connected to the firewall of the internal local area network.

Q3) Can I update my access point to this mSSID firmware?

Yes. You can retain your access point configuration when you update to the mSSID firmware if the current firmware running is v1.3x and above.

If AP is running the following configuration setup, updating to the mSSID firmware will affect the configuration.

If AP is running as PtP (Point-To-Point) or PtMP (Point-To-MultiPoint) mode. The reason it cannot retain the configuration is because mSSID uses a new PtP and PtMP connection setup method called: RootAP and Transparent Client. This method is compliant with IEEE 802.11h standard.

AP is running very old firmware v1.2x and below.

Q4) Can I update to mSSID firmware but setup only one SSID connection?

Yes, mSSID firmware operation is similar to previous single SSID firmware when setup with one SSID.

If the existing AP is running v1.3x firmware, after updating to mSSID it will retain and continue to run the previous configuration. No reconfiguration is needed.

Q5) I have a MAC Filtering table set from a previous firmware. Will updating to mSSID cause the MAC table to be lost?

No, if your firmware is v1.3x and higher, updating to mSSID firmware will retain all entries in the MAC table.

However, if you switch back from mSSID to the previous sSSID firmware, the MAC table will be lost.

Q6) I have Pseudo VLAN for Per Group enabled. Will updating to mSSID firmware still support wireless clients with MAC addresses listed in Per Group?

The mSSID firmware replaces Pseudo VLAN and integrates it into VAP (Virtual AP) and MAC Filtering.

Thus, Pseudo VLAN with its VLAN ID and MAC listing will be lost after updating to mSSID firmware.

Refer to the user manual on how to create new VAP with VLAN ID and MAC Filtering.

Similarly, Per Node (control to isolate wireless station in AP) being part of Pseudo VLAN will also be lost.

This option can be enabled again with the option "Station Isolation" in VAP setup page.

Q7) I have WDS setup in my network. Will mSSID still support this?

WDS has the limitation that it can only support WEP security key.

To support higher wireless security it is replaced with Repeater mode in mSSID firmware.

Thus, updating to mSSID will disconnect the WDS links and connections with the rest of the APs.

It is recommended to connect directly to each AP to update the firmware, then set to Repeater mode and configure it before updating the next AP. This way you can build back the connections.

Refer to the user manual for more details instructions on the setup.

Updating to the mSSID firmware is not necessary if you do not need the higher wireless security support.

Q8) I have 2 of the access point units installed at a site about 2km from each other running PtP modes.

Should I update to mSSID firmware? Can I do it from one location to update the firmware like I do with the current single SSID firmware?

The setup for PtP and PtMP for mSSID firmware is different the current sSSID firmware.

After mSSID firmware starts up, the link between the 2 APs will be lost. The recommended method is to setup 2 similar model units in the office. Load the mSSID firmware and create the new PtP / PtMP configuration using the actual parameters of the 2 units on site that you will update. After testing the connection to be working in the office, backup the configuration file for each unit.

Go to the first site to update the mSSID firmware and restore the configuration for the site, then go to the next site and do the same. When both APs are up again, the network at both sides should be connected with the new PtP setup.

** Note: If existing PtP connection is running well, it is not necessary to update to the mSSID firmware.

Unless you have the following concerns:

Current firmware PtP is not compliant with IEEE 802.11h standard and the respective country authority requires it to be changed.

Current firmware PtP wireless security only supports WEP key and you are very concerned about the vulnerability to being hacked.

Appendix: View the Technical Specifications

Safety and Electromagnetic Conformance	<ul style="list-style-type: none"> FCC Part 15 SubPart B and SubPart C (for wireless module) EN 300 328-2 EMC CE EN 301 489 (EN300 826) EN 55022 (CISPR 22)/EN 55024 Class B EN 61000-3-2 EN61000-3-3 CE EN 60950
Standards	
IEEE802.11b:	<ul style="list-style-type: none"> 11Mbps, 5.5Mbps, 2Mbps, 1Mbps
IEEE802.11g:	<ul style="list-style-type: none"> 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps, automatically fallback to 5.5Mbps, 2Mbps, 1Mbps
Super-G:	<ul style="list-style-type: none"> 108Mbps, 96Mbps, 72Mbps, 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 6Mbps
Frequency Range IEEE 802.11b/g:	2.412GHz ~ 2.462GHz (US & Canada) 2.412GHz ~ 2.472GHz (Europe) 2.412GHz ~ 2.484GHz (Japan)
Max Tx Power:	17dBm
Security	<ul style="list-style-type: none"> 64 - bit / 128 - bit WEP WPA-EAP, WPA-PSK, WPA2 Tagged VLAN IEEE 802.1x – TLS, TTLS, PEAP, EAP-SIM
Network Interface	<ul style="list-style-type: none"> 10/100 Mbps auto-negotiating Ethernet port (RJ45)
Modulation Techniques	OFDM (BPSK, QPSK, 16-QAM, 64-QAM), DSSS (BPSK, QPSK, CCK)
Operating Channels	<ul style="list-style-type: none"> 11 Channels (US and Canada) 13 Channels (Europe) 14 Channels (Japan)
Advanced Wireless Feature	<ul style="list-style-type: none"> Virtual AP Long Distance Parameters Setup Smart Select STP HTTPS
Antenna	Detachable 2dBi antenna with SMA connector
Management	<ul style="list-style-type: none"> HTTP Web Management SNMP <ul style="list-style-type: none"> - SNMP (RFC1157) - SNMP (RFC1213) Telnet SSH
Built-in DHCP Server	Yes
DHCP Reservation	By MAC address

Configuration Backup & Restore	Yes
Firmware Upgrade	Yes
Power Requirements Using Power Adapter: Using PoE:	24VDC 15-48VDC
Operating Temp:	-20°C to +70°C
Storage Temp:	-30°C to +80°C
Operating Humidity:	10% to 80% RH Humidity (RH – Relative Humidity)
Physical Dimensions	91.8mm x 66mm x 25mm (H x W x D)

© Copyright 2007 Compex Systems Pte Ltd

All Rights Reserved

This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

Trademark Information

Compex® is a registered trademark of Compex, Inc. Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. All other brand and product names are trademarks or registered trademarks of their respective owners.

Notice: Copyrights © 2007 by Compex, Inc. All rights reserved. Reproduction, adaptation, or translation without prior permission of Compex, Inc. is prohibited, except as allowed under the copyright laws.

Manual Revision by Daniel

Manual Number: U-0587-V1.1C Version 1.1 August 2007

Disclaimer

Compex, Inc. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Compex, Inc. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Compex, Inc will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

FCC NOTICE

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Connect the computer into an outlet on a circuit different from that to which the receiver is connected.
- Increase the separation between the computer and receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC Compliance Statement: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference, and

This device must accept any interference received, including interference that may cause undesired operation.

Products that contain a radio transmitter are labelled with FCC ID and may also carry the FCC logo.

Caution: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements, the following antenna installation and device operating configurations must be satisfied:

- a. For configurations using the integral antenna, the separation distance between the antenna(s) and any person's body (including hands, wrists, feet and ankles) must be at least 2.5cm (1 inch).
- b. For configurations using an approved external antenna, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20cm (8 inch).

The transmitter shall not be collocated with other transmitters or antennas.

ICES 003 Statement

This Class B digital apparatus complies with Canadian ICES-003.

Declaration of Conformity

Compex, Inc. declares the following:

Product Name: Wireless Network Access Point

Model No.: WPE53G conforms to the following Product Standards:

This device complies with the Electromagnetic Compatibility Directive (89/336/EEC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards.)

Electromagnetic Interference (Conduction and Radiation): EN 55022 (CISPR 22)

Electromagnetic Immunity: EN 55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)

Low Voltage Directive: EN 60 950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11: 1997.

Therefore, this product is in conformity with the following regional standards: FCC Class B: following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Compex, Inc. also declares that:

The wireless card in this product complies with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following:

EMC Standards: FCC: 47 CFR Part 15, Subpart B, 47 CFR Part 15, Subpart C (Section 15.247); CE: EN 300 328-2, EN 300 826 (EN 301 489-17)

Therefore, this product is in conformity with the following regional standards: FCC Class B: following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Firmware

This manual is written based on Firmware version 2

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 Centres:

Technical Support Centres	
Contact the technical support centre that services your location.	
U.S.A., Canada, Latin America and South America	
✉ Write	Compex, Inc. 840 Columbia Street, Suite B Brea, CA 92821, USA
☎ Call	Tel: +1 (714) 482-0333 (8 a.m.-5 p.m. Pacific time) Tel: +1 (800) 279-8891 (Ext.122 Technical Support)
☎ Fax	Fax: +1 (714) 482-0332
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)
☎ Fax	Tel: (65) 6286-2086 (Ext.199 Technical Support) Fax: (65) 6283-8337
Internet access	E-mail: support@compex.com.sg FTPsite: ftp.compex.com.sg
Website:	http://www.cpx.com or http://www.compex.com.sg

We value your feedback. If you have any suggestions on improving, we would like to hear from you.

Please contact us at:

Fax: (65) 62809947

Email: feedback@compex.com.sg

We hope this manual was helpful to you. For more Compex information, please visit us at www.Compex.com.sg

warning

Class B:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.