6.13 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP**, **128-bit WEP** or **152-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 16 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

6.14 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

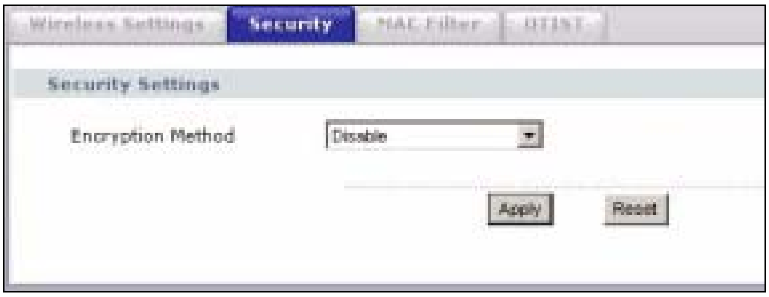
6.15 Configuring Wireless Security

In order to configure and enable wireless security; click **SETTINGS** > **WIRELESS** > **Security** to display the **Security** screen. This screen varies according to the encryption method you select.

6.15.1 Wireless Security: Disable

If you do not enable any wireless security on your device, your network is accessible to any wireless networking device that is within range.

Figure 47 Wireless Security: Disable



Security Settings

Encryption Method: Disable

The following table describes the labels in this screen.

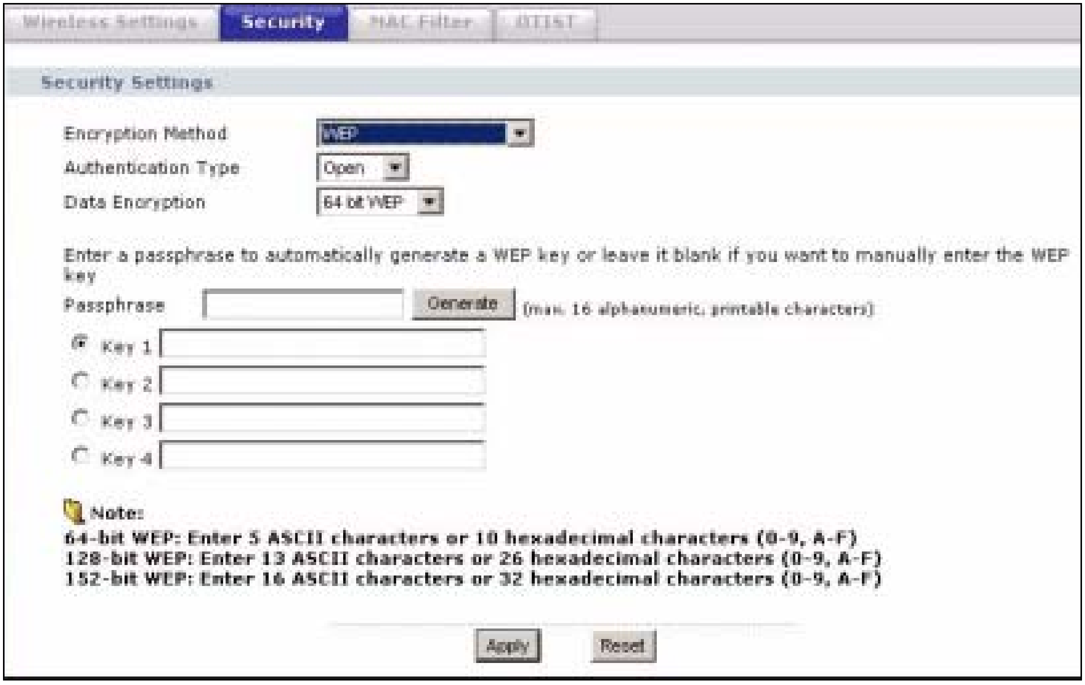
Table 17 Wireless Security: Disable

LABEL	DESCRIPTION
Encryption Method	Select **Disable** to have no wireless LAN security configured.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.15.2 Wireless Security: WEP

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. You can configure up to four 64-bit, 128-bit or 152-bit WEP keys, but only one key can be used at any one time.

Figure 48 Wireless Security: WEP



Security Settings

Encryption Method: WEP

Authentication Type: Open

Data Encryption: 64 bit WEP

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key

Passphrase: Generate (max. 16 alphanumeric, printable characters)

● Key 1

○ Key 2

○ Key 3

○ Key 4

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)

The following table describes the labels in this screen.

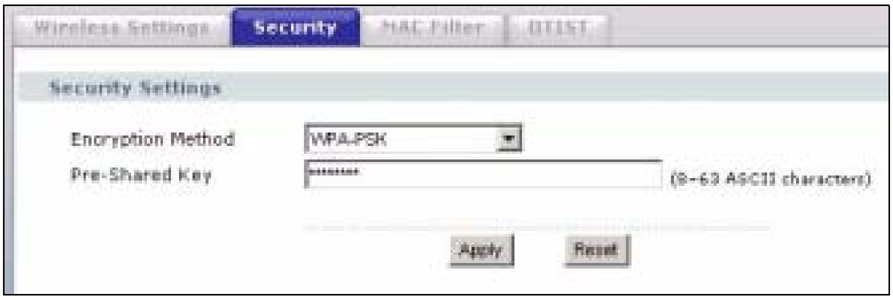
Table 18 Wireless Security: WEP

LABEL	DESCRIPTION
Encryption Method	Select **WEP** if you want to configure WEP encryption parameters.
Authentication Type	Select **Auto**, **Open** or **Shared** from the drop-down list box.
WEP Encryption	Select **64 bit WEP**, **128 bit WEP** or **152 bit WEP** to enable data encryption.
Passphrase	If you selected 64-bit or 128-bit WEP, you can enter a “passphrase” (password phrase) of up to 32 case-sensitive printable characters and click **Generate** to have the device create four different WEP keys.
Generate	After you enter the passphrase, click **Generate** to have the device generates four different WEP keys automatically.
Key 1 to Key 4	If you want to manually set the WEP keys, enter the WEP key in the field provided. Select a WEP key to use for data encryption. The WEP keys are used to encrypt data. Both the device and the wireless stations must use the same WEP key for data transmission. If you chose **64 bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128 bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **152 bit WEP**, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F").
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.15.3 Wireless Security: WPA(2)-PSK

Select **WPA-PSK**, **WPA2-PSK** or **WPA-PSK & WPA2-PSK** in the **Encryption Method** drop down list-box to display the screen displays as next.

Figure 49 Wireless Security: WPA(2)-PSK



Security Settings

Encryption Method: WPA-PSK

Pre-Shared Key: ******** (8-63 ASCII characters)

The following table describes the labels in this screen.

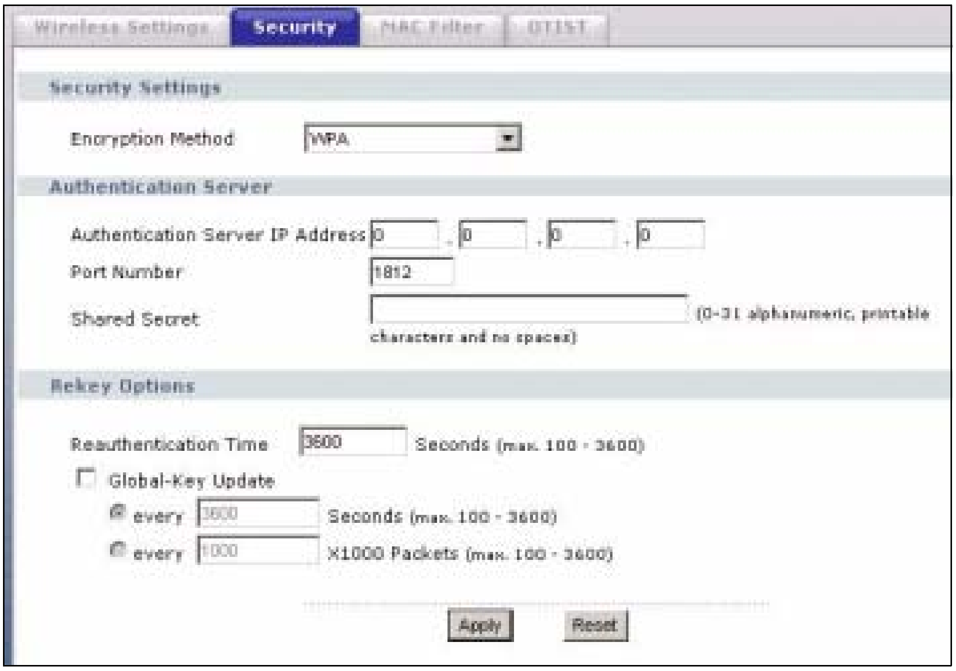
Table 19 Wireless Security: WPA-PSK

LABEL	DESCRIPTION
Encryption Method	Select **WPA-PSK**, **WPA2-PSK** or **WPA-PSK & WPA2-PSK** if you want to configure a pre-shared key. Choose this option only if your wireless clients support it.
Pre-Shared Key	The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). This field is case-sensitive.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.15.4 Wireless Security: WPA(2)

WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are user authentication and improved data encryption.

Figure 50 Wireless Security: WPA(2)



Security Settings

Encryption Method WPA

Authentication Server

Authentication Server IP Address 0 . 0 . 0 . 0

Port Number 1812

Shared Secret (0-31 alphanumeric, printable characters and no spaces)

Rekey Options

Reauthentication Time 3600 Seconds (max. 100 - 3600)

□ Global-Key Update

● every 3600 Seconds (max. 100 - 3600)

○ every 1000 X1000 Packets (max. 100 - 3600)

The following table describes the labels in this screen.

Table 20 Wireless Security: WPA(2)

LABEL	DESCRIPTION
Encryption Method	Select **WPA**, **WPA2** or **WPA & WPA2** to configure user authentication and improved data encryption. **Note:** WPA, WPA2 and IEEE 802.1x wireless security are not available when you use Wireless Client, Bridge or AP+Repeater mode. You can only use WEP keys to encrypt traffic between APs.
Authentication Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 63 printable characters) as the key to be shared between the external authentication server and the device. The key must be the same on the external authentication server and your device. The key is not sent over the network.
Reauthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 100 and 3600 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

Table 20 Wireless Security: WPA(2) (continued)

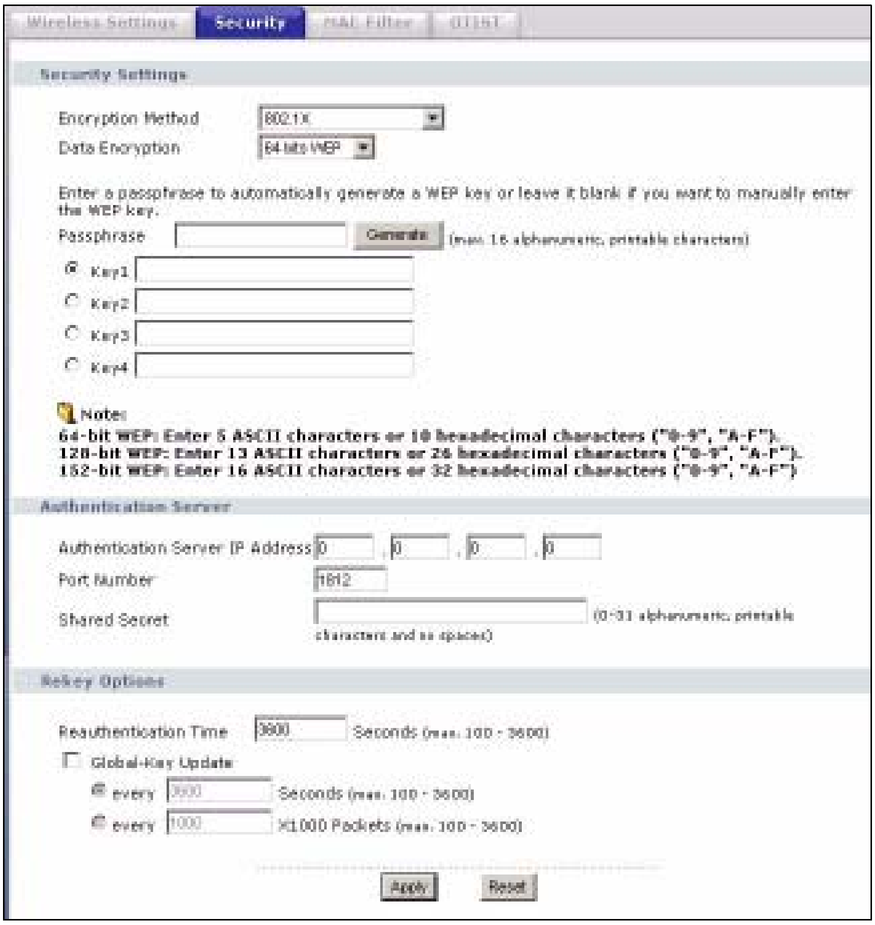
LABEL	DESCRIPTION
Global-Key Update	This is how often the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Specify an interval either in seconds or thousands of packets that the device sends.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.15.5 Wireless Security: IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management.

Note: Once you enable user authentication, you need to specify an external RADIUS server on the device for authentication.

Figure 51 Wireless Security: 802.1x



Security Settings

Encryption Method: 802.1X

Data Encryption: 64 bits WEP

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key.

Passphrase: (max. 16 alphanumeric, printable characters)

● Key1
○ Key2
○ Key3
○ Key4

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F")

Authentication Server

Authentication Server IP Address: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret: (0-31 alphanumeric, printable characters and no spaces)

Rekey Options

Reauthentication Time: 3600 Seconds (max. 100 - 3600)

□ Global-Key Update

● every 3600 Seconds (max. 100 - 3600)

○ every 1000 X1000 Packets (max. 100 - 3600)

The following table describes the labels in this screen.

Table 21 Wireless Security: 802.1x

LABEL	DESCRIPTION
Encryption Method	Select **802.1X** to configure authentication of wireless stations and encryption key management. **Note:** WPA, WPA2 and IEEE 802.1x wireless security are not available when you use Bridge or AP+Repeater mode. You can only use WEP keys to encrypt traffic between APs.
Data Encryption	Select **None** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64 bits WEP**, **128 bits WEP** or **152 bits WEP** to enable data encryption. Up to 32 stations can access the device when you configure dynamic WEP key exchange.
Authentication Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 63 printable characters) as the key to be shared between the external authentication server and the device. The key must be the same on the external authentication server and your device. The key is not sent over the network.
Reauthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 100 and 3600 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Global-Key Update	This is how often the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Specify an interval either in seconds or thousands of packets that the device sends.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.16 MAC Filter

The MAC filter screen allows you to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the device (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

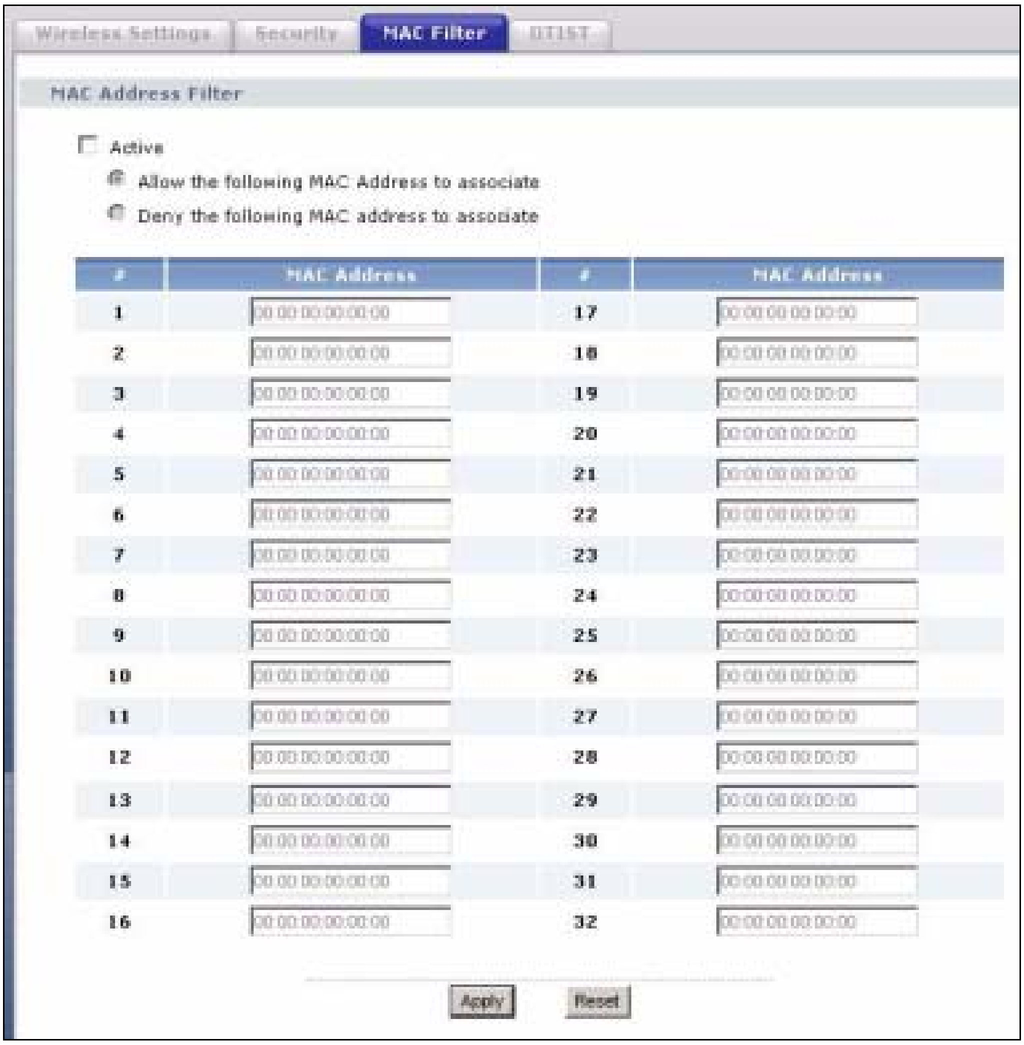
The MAC filter works when the device functions as an AP. It allows or denies wireless client access. The MAC filter does not apply to bridge or repeater functions.

The following applies if you set the device to client mode and want to connect to an AP that uses a MAC filter. After the device turns on in client mode, it clones the MAC address of the first packets that it receives from devices connected to the Ethernet port. It uses this MAC address on the packets that it sends to an AP. All of the packets that the device sends to an AP will appear to be from the first device that connected to the Ethernet port. If you turn the device off and back on, it again clones the MAC address of the first packets that it receives from devices connected to the Ethernet port. You may be able to check the association list on the AP to determine which MAC address the device is currently using.

To change your device's MAC filter settings, click **WIRELESS** > **SETTINGS** > **MAC Filter**. The screen appears as shown.

Note: Be careful not to list your computer's MAC address and select **Deny the following MAC address to associate** when managing the device via a wireless connection. This would lock you out.

Figure 52 MAC Filter



MAC Address Filter

□ Active

● Allow the following MAC Address to associate

○ Deny the following MAC address to associate

#	MAC Address	#	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 22 MAC Filter

LABEL	DESCRIPTION
Active	Select the check box to enable MAC address filtering and define the filter action for the list of MAC addresses in the MAC address filter table. Select **Allow the following MAC address to associate** to permit access to the device, MAC addresses not listed will be denied access to the device. Select **Deny the following MAC address to associate** to block access to the device, MAC addresses not listed will be allowed to access the device.
#	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the device in these address fields.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.17 OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as “AP” here) in order to associate with it. Traditionally this meant that you had to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP’s SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA-PSK key for you if you didn’t configure one manually.

Note: OTIST replaces the pre-configured wireless settings on the wireless clients.

6.17.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

Note: The AP and wireless client(s) MUST use the same **Setup key**.

6.17.1.1 AP

You can enable OTIST using the **OTIST** button or the web configurator.

6.17.1.1.1 OTIST Button

If you use the **OTIST** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used to encrypt the settings that you want to transfer.

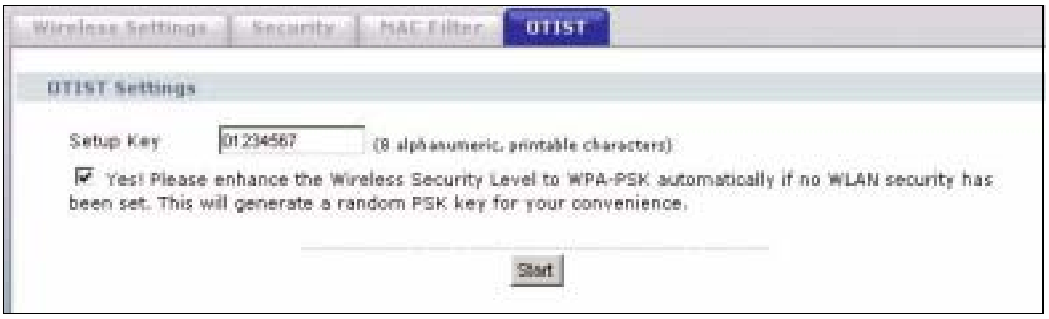
Hold in the **OTIST** button for one or two seconds.

6.17.1.1.2 Web Configurator

Click **WIRELESS** > **SETTINGS** > **OTIST** to configure and enable OTIST. The screen appears as shown.

Note: At the time of writing the device does not support OTIST in the wireless client mode.

Figure 53 OTIST



OTIST Settings

Setup Key 01234567 (8 alphanumeric, printable characters)

☑ Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience.

The following table describes the labels in this screen.

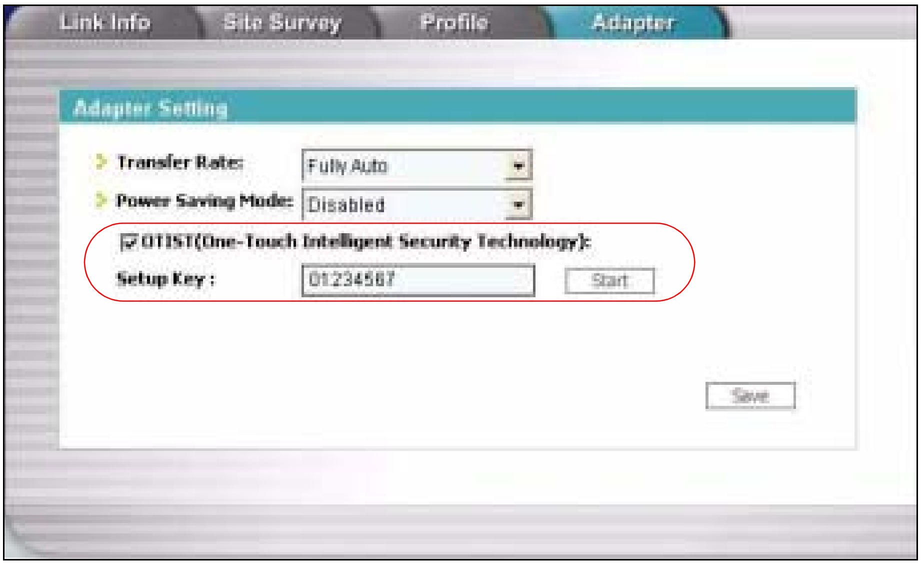
Table 23 OTIST

LABEL	DESCRIPTION
One-Touch Intelligent Security Technology	
Setup Key	Enter the setup key of up to eight printable characters. The default OTIST setup key is "01234567". **Note:** If you change the OTIST setup key here, you must also make the same change on the wireless client(s).
Yes!	To have OTIST automatically generate a WPA-PSK key, select this check box. If you manually configured a WEP key or a WPA-PSK key and you also select this check box, then the key you manually configured is used.
Start	Click **Start** to encrypt the wireless security data using the setup key and have the device set the wireless client to use the same wireless settings as the device. You must also activate and start OTIST on the wireless client at the same time. The process takes three minutes to complete.

6.17.1.2 Wireless Client

Start the ZyXEL utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP’s and click **Save**.

Figure 54 Example Wireless Client OTIST Screen



Adapter Setting

Transfer Rate: Fully Auto

Power Saving Mode: Disabled

☑ OTIST(One-Touch Intelligent Security Technology):

Setup Key : 01234567 Start

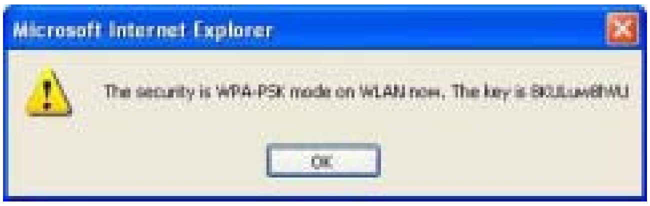
Save

6.17.2 Starting OTIST

Note: You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

1 In the AP, a web configurator screen pops up showing you the security settings to transfer. After reviewing the settings, click **OK**.

Figure 55 Security Key



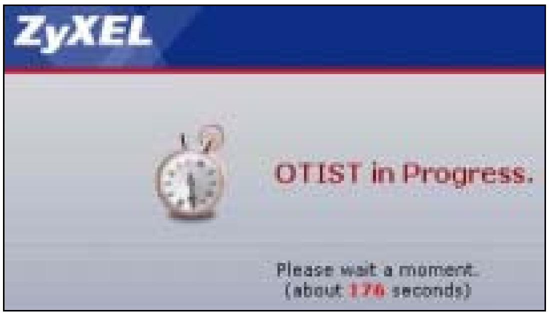
Microsoft Internet Explorer

The security is WPA-PSK mode on WLAN now, The key is 8KULuw8hWU

OK

2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.

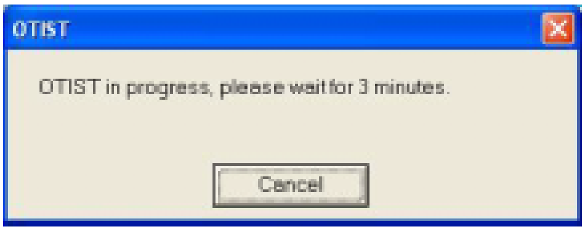
Figure 56   OTIST in Progress (AP)



OTIST in Progress.

Please wait a moment.
(about 176 seconds)

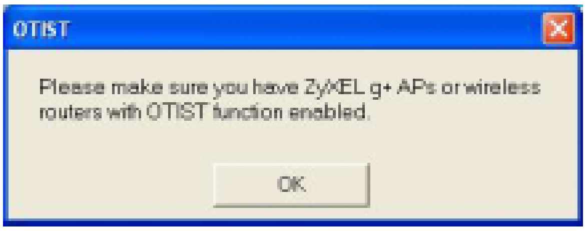
Figure 57   OTIST in Progress (Client)



OTIST in progress, please wait for 3 minutes.

- In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same**Setupkey**).Click**OK**togobacktotheZyXELutilitymainscreen.

Figure 58   No AP with OTIST Found



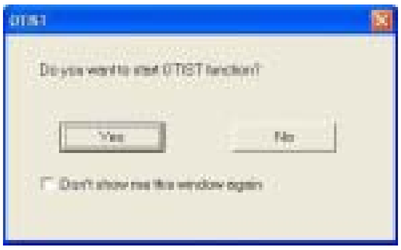
Please make sure you have ZyXEL g+ APs or wireless routers with OTIST function enabled.

- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

6.17.3 Notes on OTIST

1 If you enabled OTIST in the wireless client, you see this screen each time you start the utility. Click **Yes** for it to search for an OTIST-enabled AP.

Figure 59 Start OTIST?



Do you want to start OTIST function?

□ Don't show me this window again

2 If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)

3 When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP **OTIST** web configurator screen or hold in the **OTIST** button (for one or two seconds) for the AP to transfer settings.

4 If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).

5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL wireless clients again.

CHAPTER 7
Management Screens

This chapter describes the Maintenance screens.

7.1 Maintenance Overview

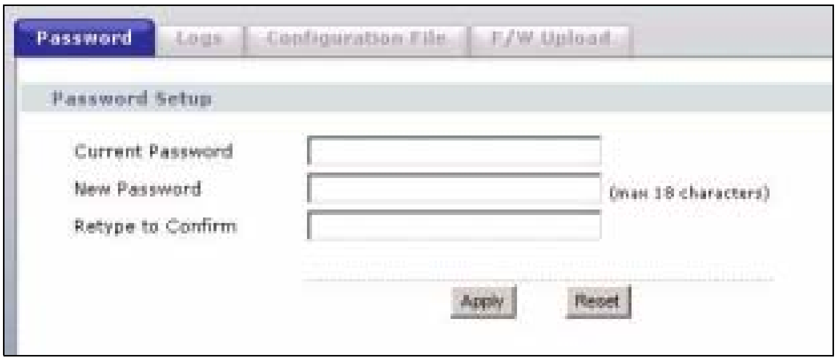
Use these maintenance screens to change the password, view logs, back up or restore the G-570S configuration and change the web configurator language.

7.2 Password

To change your device's password (recommended), click **SETTINGS > MANAGEMENT**. The screen appears as shown. This screen allows you to change the device's password.

If you forget your password (or the device IP address), you will need to reset the device. See the section on resetting the device for details.

Figure 60 Management: Password



Current Password
New Password (max 18 characters)
Retype to Confirm

The following table describes the labels in this screen.

Table 24 Management: Password

LABEL	DESCRIPTION
Current Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 30 printable characters). Spaces are not allowed. Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.

Table 24 Management: Password (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

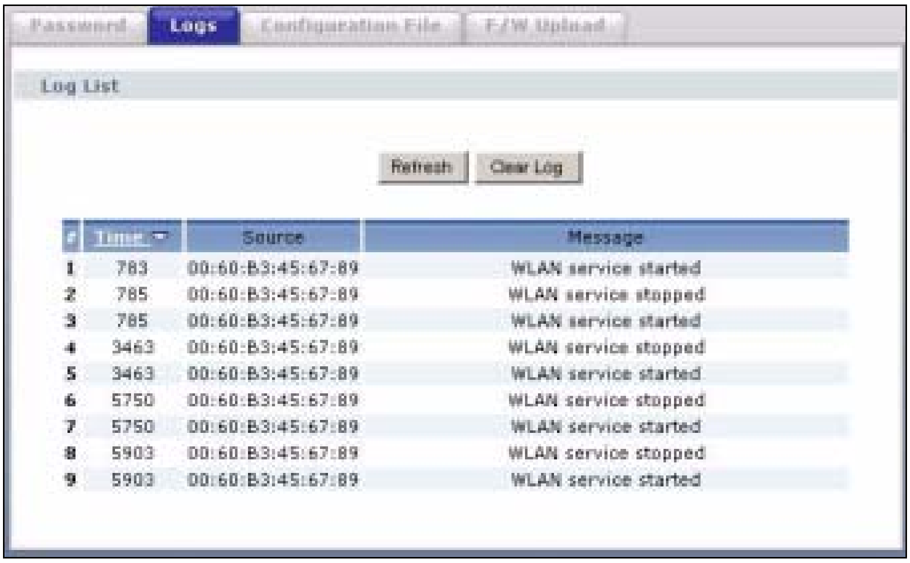
7.3 Logs

Click **SETTINGS** > **MANAGEMENT** > **Logs** to open the **Logs** screen.

You can view logs and alert messages in this screen. Once the log table is full, old logs are deleted as new logs are created.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

Figure 61 Management: Logs



#	Time	Source	Message
1	783	00:60:B3:45:67:89	WLAN service started
2	785	00:60:B3:45:67:89	WLAN service stopped
3	785	00:60:B3:45:67:89	WLAN service started
4	3463	00:60:B3:45:67:89	WLAN service stopped
5	3463	00:60:B3:45:67:89	WLAN service started
6	5750	00:60:B3:45:67:89	WLAN service stopped
7	5750	00:60:B3:45:67:89	WLAN service started
8	5903	00:60:B3:45:67:89	WLAN service stopped
9	5903	00:60:B3:45:67:89	WLAN service started

The following table describes the labels in this screen.

Table 25 Management: Logs

LABEL	DESCRIPTION
Display	Select a category of logs to view.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.
#	This is the log’s index number.
Time	This field displays the time the log was recorded. It is the number of seconds since the last time the system turned on.
Message	This field states the reason for the log.

Table 25 Management: Logs (continued)

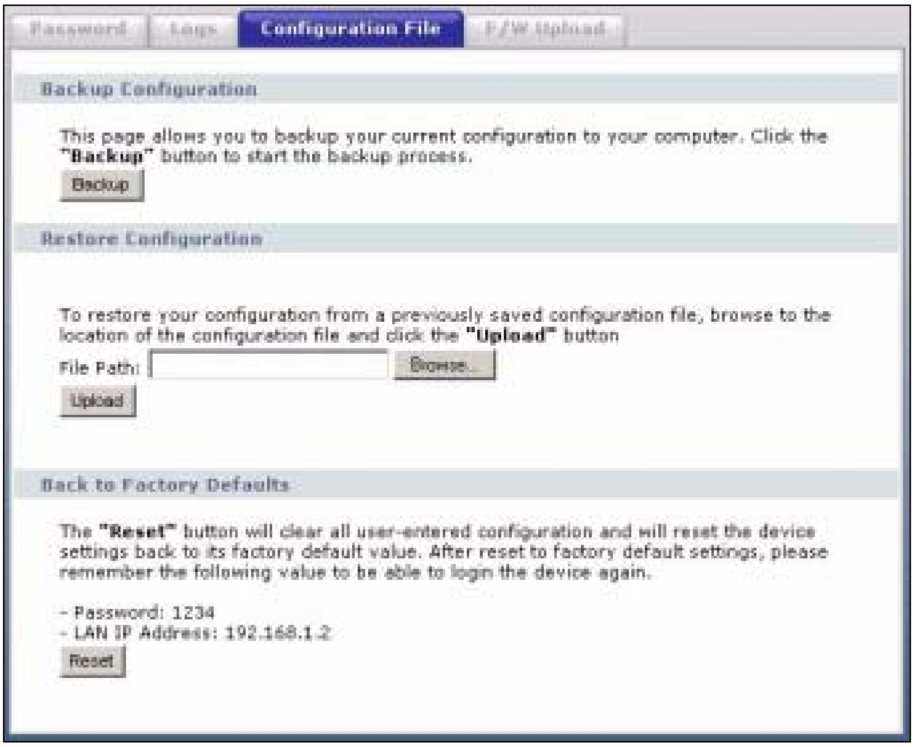
LABEL	DESCRIPTION
Source	This field lists the source IP address and the port number of the incoming packet that caused the log.
Destination	This field lists the destination IP address and the port number of the outgoing packet that caused the log.
Note	This field displays additional information about the log entry.

7.4 Configuration File

The configuration file (often called the romfile or rom-0) contains the factory default settings such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a .rom filename extension. Once you have customized the device's settings, they can be saved back to your computer under a filename of your choosing.

Click **SETTINGS** > **MANAGEMENT** > **Configuration File**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 62 Management: Configuration File



Backup Configuration

This page allows you to backup your current configuration to your computer. Click the "**Backup**" button to start the backup process.

Restore Configuration

To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the "**Upload**" button

File Path:

Back to Factory Defaults

The "**Reset**" button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following value to be able to login the device again.

- Password: 1234
- LAN IP Address: 192.168.1.2

7.4.1 Backup Configuration

Backup configuration allows you to back up (save) the device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the device's current configuration to your computer.

7.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your device.

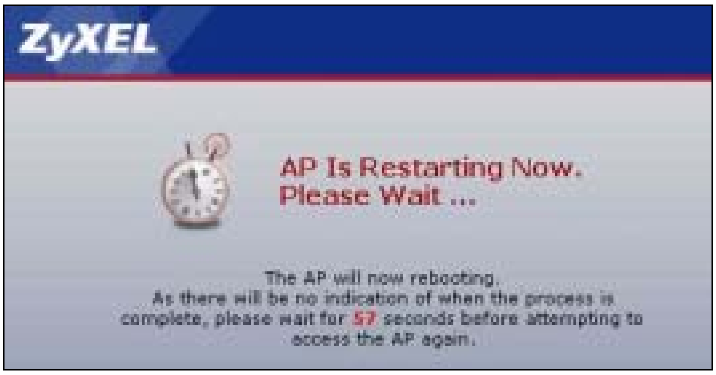
Table 26 Management: Configuration File: Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Note: Do not turn off the device while configuration file upload is in progress.

The following screen displays. You must wait one minute before logging into the device again.

Figure 63 Configuration Upload Successful

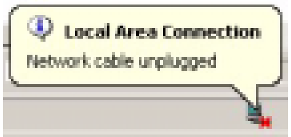


AP Is Restarting Now.
Please Wait ...

The AP will now rebooting.
As there will be no indication of when the process is complete, please wait for 57 seconds before attempting to access the AP again.

The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 64 Network Temporarily Disconnected



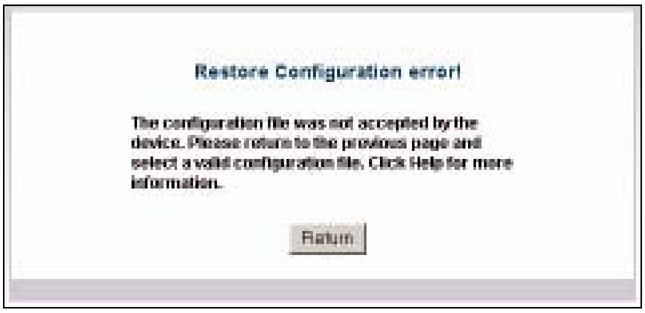
Local Area Connection

Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.2).

If the upload was not successful, the following screen will appear. Click **Return** to go back to the Configuration File screen.

Figure 65 Configuration Upload Error



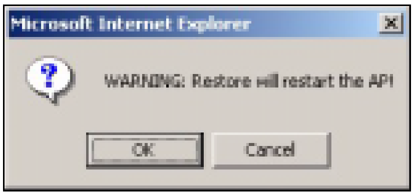
Restore Configuration error!

The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.

7.4.3 Back to Factory Defaults

Clicking the **RESET** button in this section clears all user-entered configuration information and returns the device to its factory defaults. The following warning screen will appear.

Figure 66 Reset Warning Message



Microsoft Internet Explorer

WARNING: Restore will restart the AP!

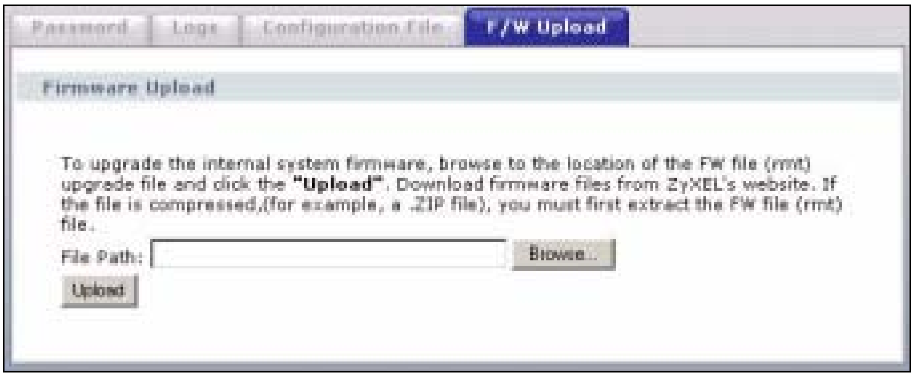
You can also press the **RESET** button on the rear panel to reset the factory defaults of your device. Refer to the section on resetting the device for more information on the **RESET** button.

7.5 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .rmt extension, for example, "zyxel.rmt". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **SETTINGS** > **MANAGEMENT** > **F/W Upload** to display the screen as shown. Follow the instructions in this screen to upload firmware to your device.

Figure 67 Management: F/W Upload



Firmware Upload

To upgrade the internal system firmware, browse to the location of the FW file (rmt) upgrade file and click the **"Upload"**. Download firmware files from ZyXEL's website. If the file is compressed,(for example, a .ZIP file), you must first extract the FW file (rmt) file.

File Path:

The following table describes the labels in this screen.

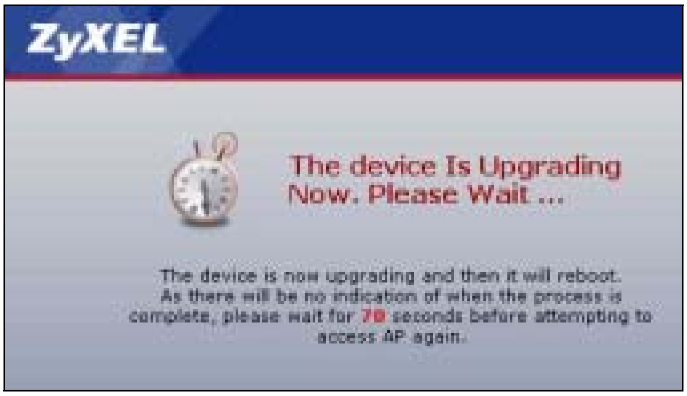
Table 27 Management: F/W Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .rmt file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the device while firmware upload is in progress!

The following screen appears. Wait two minutes before logging into the device again.

Figure 68 Firmware Upgrading Screen

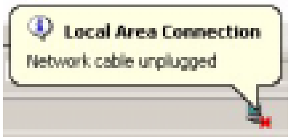


The device Is Upgrading Now. Please Wait ...

The device is now upgrading and then it will reboot. As there will be no indication of when the process is complete, please wait for 70 seconds before attempting to access AP again.

The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 69 Network Temporarily Disconnected

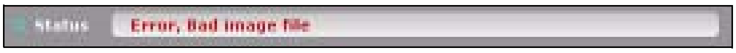


Local Area Connection
Network cable unplugged

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following status message displays at the bottom of the screen.

Figure 70 Firmware Upload Error



Status Error, Bad image file

CHAPTER 8 Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem.

8.1 Problems Starting Up the G-570S

Table 28 Troubleshooting the Start-Up of Your G-570S

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I plug in the power adaptor.	Make sure you are using the supplied power adaptor and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.
The G-570S reboots automatically sometimes.	The supplied power to the G-570S is too low. Check that the G-570S is receiving enough power. Make sure the power source is working properly.

8.2 Problems with the Password

Table 29 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the G-570S.	The **Password** field is case-sensitive. Make sure that you enter the correct password using the proper casing. Use the **RESET** button on the rear panel of the G-570S to restore the factory default configuration file (hold this button in for about 10 seconds or release the button when the **PWR** LED starts blinking). This will restore all of the factory defaults including the password.

8.3 Problems with the WLAN Interface

Table 30 Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the G-570S from the WLAN.	Make sure the wireless adapter on the wireless station is working properly. Check that both the G-570S and your wireless station are using the same ESSID, channel and security settings.
I cannot ping any computer on the WLAN.	Make sure the wireless adapter on the wireless station(s) is working properly. Check that both the G-570S and wireless station(s) are using the same ESSID, channel and security settings.

8.4 Problems with the Ethernet Interface

Table 31 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the G-570S from the LAN.	If the **ETHN** LED on the front panel is off, check the Ethernet cable connection between your G-570S and the Ethernet device connected to the **ETHERNET** port. Check for faulty Ethernet cables. Make sure your computer’s Ethernet adapter is installed and working properly. Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the G-570S, the Ethernet device and your computer are on the same subnet.
I cannot ping any computer on the LAN.	If the **ETHN** LED on the front panel is off, check the Ethernet cable connections between your G-570S and the Ethernet device. Check the Ethernet cable connections between the Ethernet device and the LAN computers. Check for faulty Ethernet cables. Make sure the LAN computer’s Ethernet adapter is installed and working properly. Verify that the IP address and the subnet mask of the G-570S, the Ethernet device and the LAN computers are on the same subnet.

Table 31 Troubleshooting the Ethernet Interface (continued)

PROBLEM	CORRECTIVE ACTION
Cannot access the web configurator.	Your computer’s and the G-570S’s IP addresses must be on the same subnet for LAN access. If you changed the G-570S’s IP address, then enter the new one as the URL. If you don’t know the G-570S’s IP address, type the device name of your G-570S as the URL. ZyXELXXXX is the default where “XXXX” is the last four digits of the MAC address. The MAC address is on the bottom of the device). If you just changed the G-570S’s IP address, your computer’s cache of machine names may contain an entry that maps the name of the G-570S to its previous IP address. In Windows, use **nbtstat -R** at the command prompt to delete all entries in your computer’s cache of machine names. Open a new browser window. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.
	You may also need to clear your Internet browser’s cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Option**s screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it. If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer’s ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device’s MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer’s ARP table. Open a new browser window.

8.4.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

8.4.1.1 Internet Explorer Pop-up Blockers

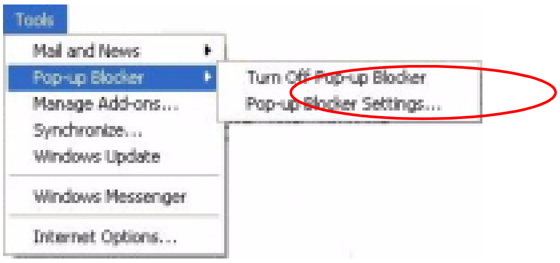
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device’s IP address.

8.4.1.1.1 Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 71 Pop-up Blocker

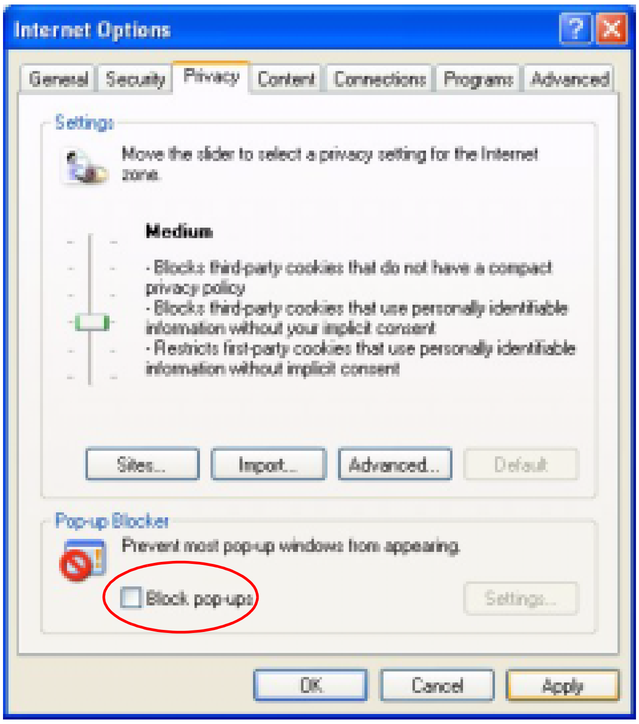


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 72 Internet Options



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

3 Click **Apply** to save this setting.

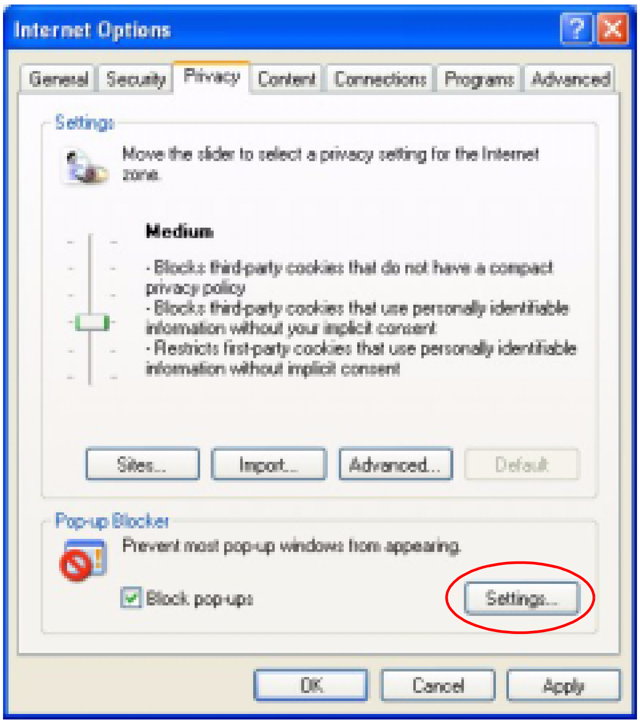
8.4.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 73 Internet Options

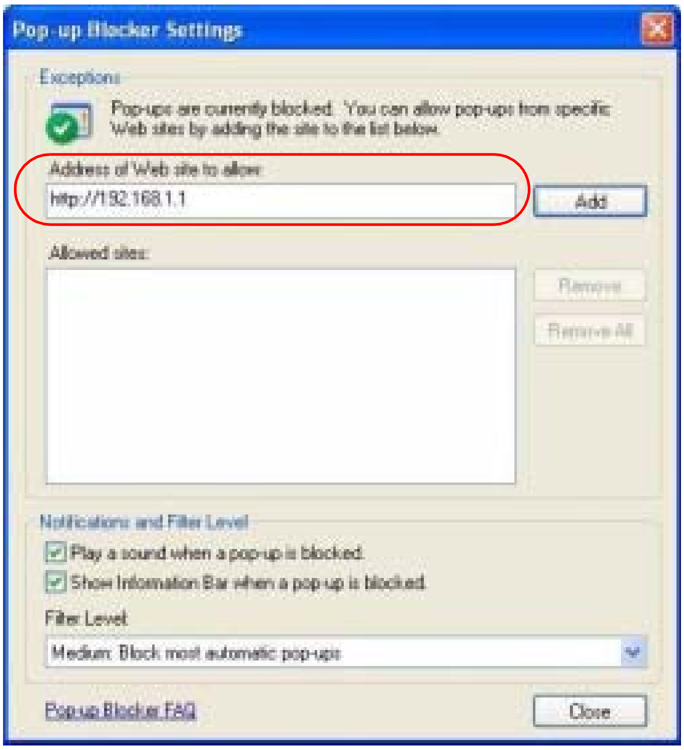


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Move the slider to select a privacy setting for the Internet zone.
Medium
- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent
Sites...
Import...
Advanced...
Default
Pop-up Blocker
Prevent most pop-up windows from appearing.
☑ Block pop-ups
Settings...
OK
Cancel
Apply

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 74 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

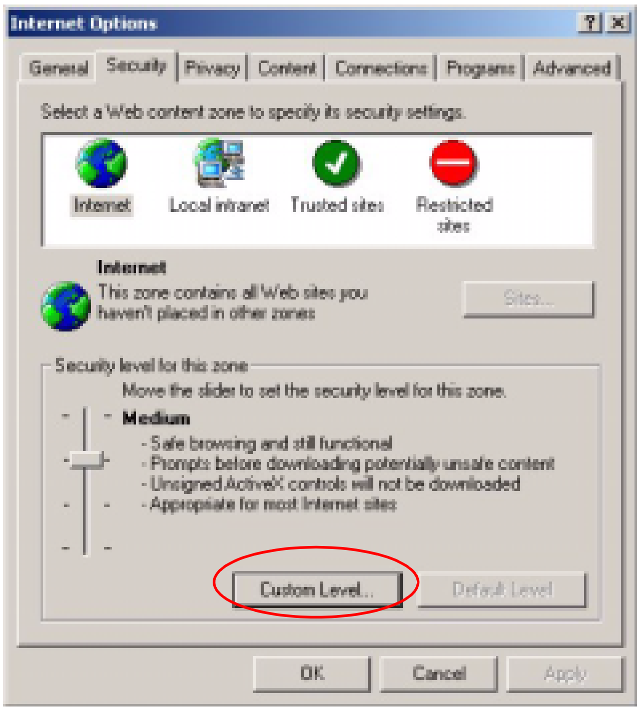
6 Click **Apply** to save this setting.

8.4.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 75 Internet Options



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

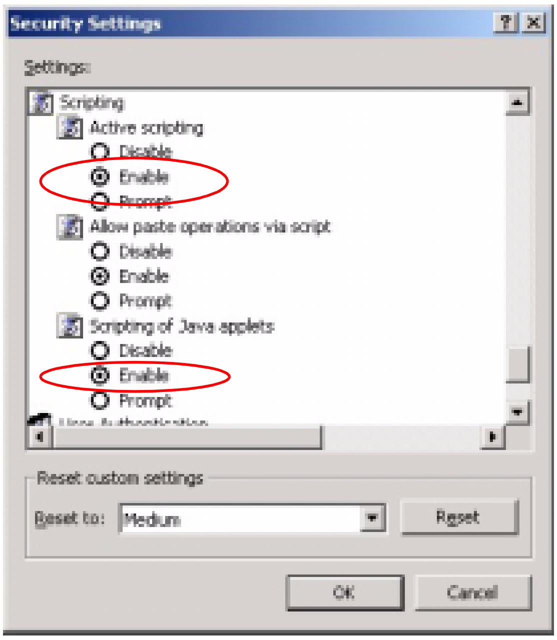
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 76 Security Settings - Java Scripting



Security Settings

Settings:

Scripting

Active scripting
- ○ Disable
- ● Enable
- ○ Prompt

Allow paste operations via script
- ○ Disable
- ● Enable
- ○ Prompt

Scripting of Java applets
- ○ Disable
- ● Enable
- ○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

8.4.1.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

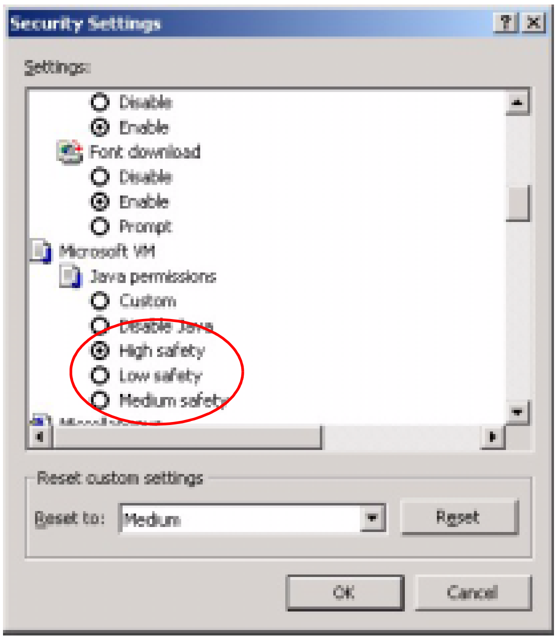
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 77 Security Settings - Java



Settings:

- ○ Disable
- ● Enable
- Font download
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Microsoft VM
  - Java permissions
    - ○ Custom
    - ○ Disable Java
    - ● High safety
    - ○ Low safety
    - ○ Medium safety

Reset to: Medium

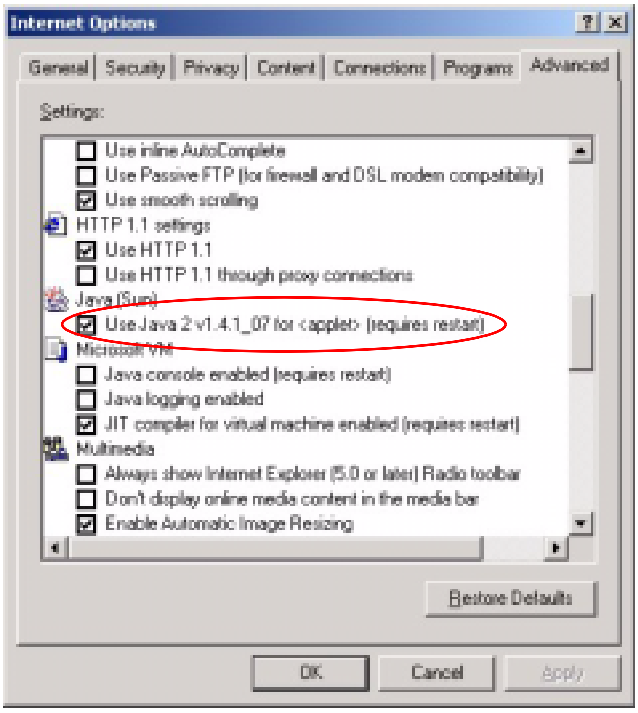
8.4.1.3.1 JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 78 Java (Sun)



- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- □ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- □ Java console enabled (requires restart)
- □ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

- □ Always show Internet Explorer (5.0 or later) Radio toolbar
- □ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

8.5 Testing the Connection to the G-570S

1. Click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ping" followed by a space and the IP address of the G-570S (192.168.1.2 is the default).
3. Press **ENTER**. The following screen displays.

Figure 79 Pinging the G-650

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2m
```

Your computer can now communicate with the G-570S via the **ETHERNET** port.

APPENDIX A
Product Specifications

See also the introduction chapter for a general overview of the key features.

Specification Tables

Table 32 Device Specifications

Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Dimensions	112 mm (Wide) × 106 mm (Deep) × 28.5 mm (High)
Weight	203 g
Ethernet Port	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Antenna	1 detachable dipole antenna
Power Requirements	12VDC @ 1 Amp maximum
Operation Temperature	0º C ~ 50º C
Storage Temperature	-30º ~ 60º C
Operation Humidity	20% ~ 95% RH
Storage Humidity	20% ~ 95% RH

Table 33 Feature Specifications

Protocol Support	Transparent bridging for unsupported network layer protocols DHCP Client DHCP relay
Standard Compliance	IEEE 802.3 and 802.3u 10Base-T and 100Base-TX physical layer specification IEEE 802.11g specification compliance for wireless LAN IEEE 802.11b specification compliance for wireless LAN IEEE 802.1x security standard support Wi-Fi certificate
Roaming	IEEE 802.11g compliant IEEE 802.11b compliant IEEE 802.11f partially compliant (without re-authentication)

Table 33 Feature Specifications (continued)

Operating Modes	Access Point Client Bridge Access Point and Repeater
Wireless Links	Up to four bridge links. Two or more repeater links are supported. It is suggested that you only use up to three repeater links.
Management	Embedded Web Configurator Command-line interface Telnet support (Password-protected telnet access to internal configuration manager). FTP//Web for firmware downloading and configuration backup and restore. Limitation of client connections (# is configurable, default: unlimited) Intra BSS Block (enable/disable) Output Power Management (4-levels)
Security	WPA and IEEE 802.1x security (EAP-TLS, EAP-TTLS, LEAP,. EAP-PEAP and Win XP PEAP included) 64/128/152-bits WEP WPA/WPA2 support based on 802.11i standard Dynamic WEP key exchange MAC address filtering through WLAN (supports up to 32 MAC address entries AES Support
Diagnostics Capabilities	Built-in Diagnostic Tools for FLASH memory, RAM, Ethernet port and wireless port. Syslog Error log Trace Log Packet Log
Hardware Features	Restore Factory Defaults (reset) Button Status LEDs • PWR • ETHN • OTIST • WLAN

Table 34 Wireless RF Specifications

STANDARD	IEEE802.11 COMPLIANCE
Data Rate	Super G/11g: 108M/54M/48M/36M/24M/18M/12M/9/6 Mbps auto fallback 11b: 11Mbps/5.5Mbps/2Mbps/1Mbps auto fallback
Communication Method	Half Duplex
Transmission/Emission Type	Direct Sequence Spread Spectrum (DSSS)

Table 34 Wireless RF Specifications

STANDARD	IEEE802.11 COMPLIANCE
Security	Wired Equivalent Privacy (WEP) data encryption Dynamic WEP key exchange WiFi Protected Access (WPA) IEEE 802.1x
RF frequency range	2.412~2.462GHz: North America 2.412MHz~2.484 GHz: Japan 2.412-2.472 GHz: Europe ETSI
Data modulation type	OFDM/BPSK/QPSK/CCK/PBCC/DQPSK/DBPSK
Peak Output Power	11b: 17.32 dBm 11g: 21.48 dBm Turbo mode: 22.25 dBm
Sensitivity	54M: -65dBm 11M: -80dBm
Coverage	Indoor: up to 100meters Outdoor: up to 400meters
Antenna	1 external detachable 2.05dBi dipole antenna with R-SMA connector

Approvals

Table 35 Approvals

SAFETY	North America	ANSI/UL-1950 3rd CSA C22.2 No. 950 3rd
	European Union (CE mark)	EN60950 (1992+A1+A2+A3+A4+A11) IEC 60950 3rd
EMI	North America	FCC Part 15 Class B
	European Union (CE mark)	EN55022 Class B EN61000-3-2 EN61000-3-3
EMS	European Union (CE mark)	
ELECTROSTATIC DISCHARGE		EN61000-4-2
RADIO-FREQUENCY ELECTROMAGNETIC FIELD		EN61000-4-3
EFT/BURST		EN61000-4-4
SURGE		EN61000-4-5
CONDUCTED SUSCEPTIBILITY		EN61000-4-6
POWER MAGNETIC		EN61000-4-8

Table 35 Approvals (continued)

VOLTAGE DIPS/ INTERRUPTION		EN61000-4-11
EM FIELD FROM DIGITAL TELEPHONES		ENV50204
LAN COMPATIBILITY		SmartBit
FOR WIRELESS PC CARD		FCC Part15C, Sec15.247
		ETS300 328 ETS300 826
		CE mark

Power Adaptor Specifications

Table 36 Power Adaptor Specifications

AUSTRALIAN PLUG STANDARDS	
AC Power Adapter Model	AD-121AE
Input Power	240 Volts AC 50Hz
Output Power	12 Volts DC ±5% 1 Amp
Power Consumption	12 Watts
Safety Standards	C-Tick
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	AD-121AB
Input Power	230 Volts AC 50Hz
Output Power	12 Volts DC ±5%, 1 Amp
Power Consumption	12 Watts
Safety Standards	CE mark, EN60950 (2001)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	AD-121A
Input Power	120 Volts AC 60Hz
Output Power	12 Volts DC ±5%, 1 Amp
Power Consumption	12 Watts
Safety Standards	UL
UK PLUG STANDARDS	
AC Power Adapter Model	AD-121AD
Input Power	240 Volts AC 50Hz
Output Power	12 Volts DC ±5% 1 Amp

Table 36 Power Adaptor Specifications (continued)

Power Consumption	12 Watts
Safety Standards	CE mark, EN60950 (2001)

APPENDIX B
Setting up Your Computer’s IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

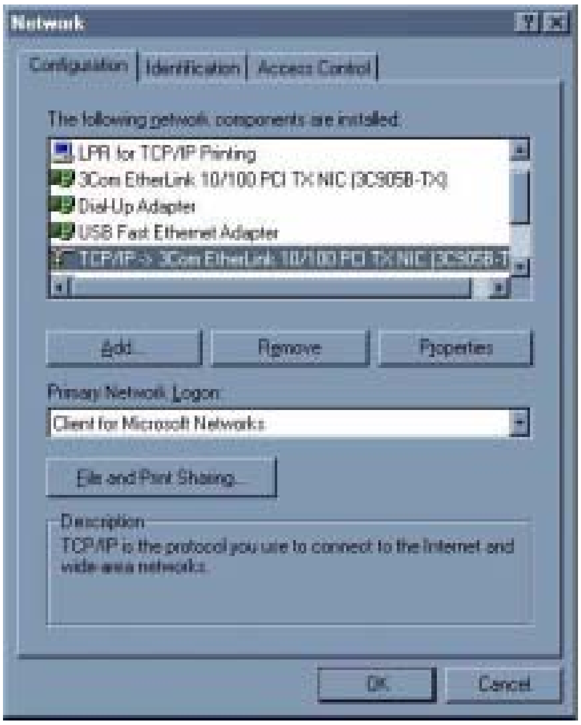
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the G-570S’s LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 80 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

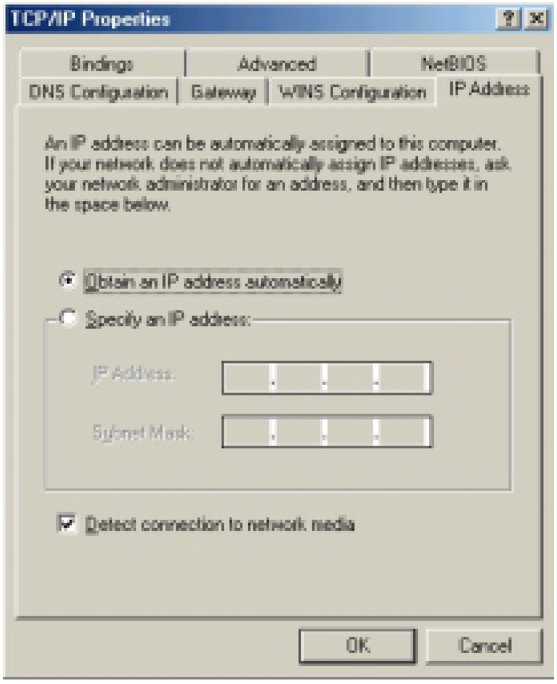
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 81 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

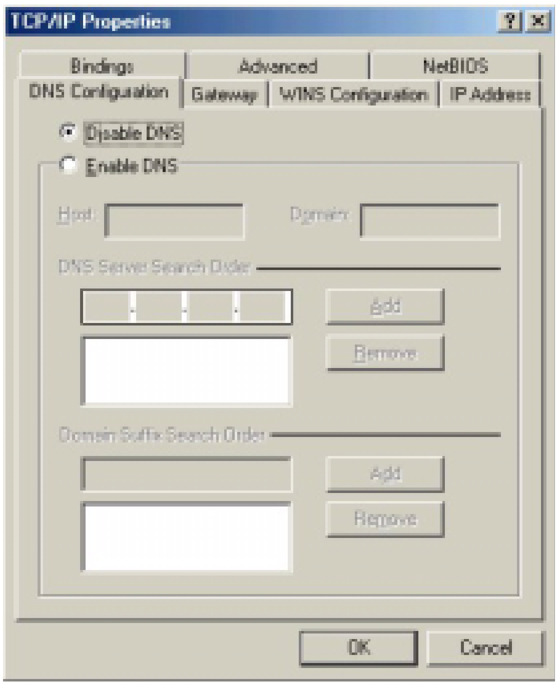
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 82 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway’s IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your G-570S and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

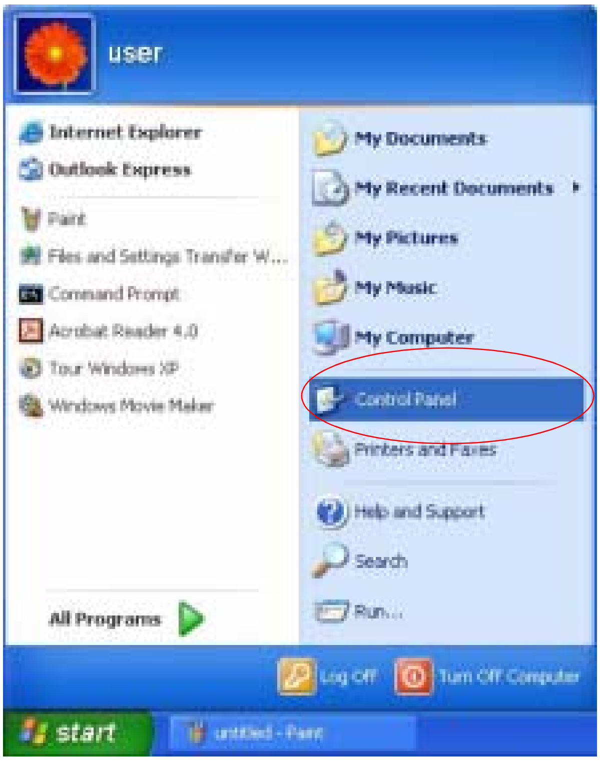
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

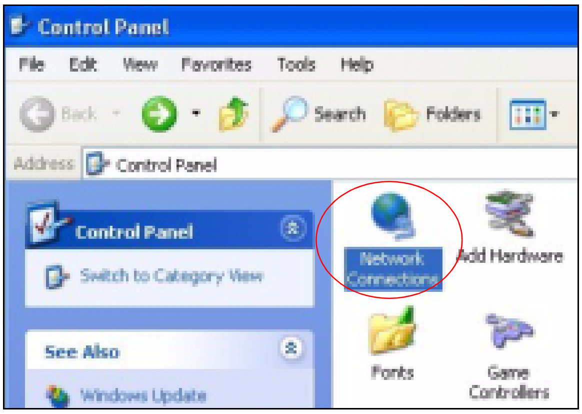
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 83 Windows XP: Start Menu



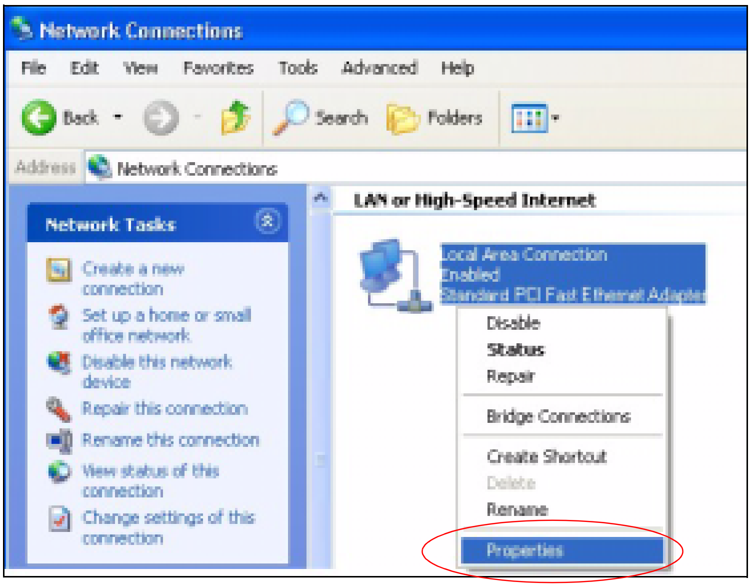
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 84 Windows XP: Control Panel



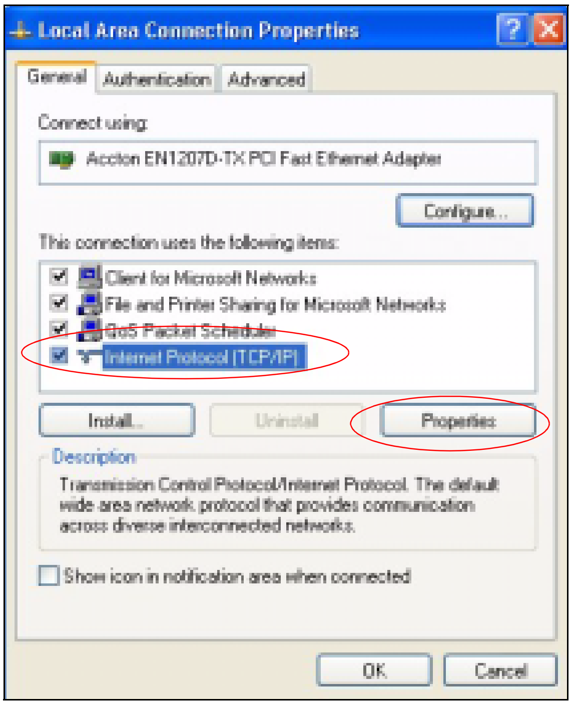
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 85 Windows XP: Control Panel: Network Connections: Properties


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 86 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

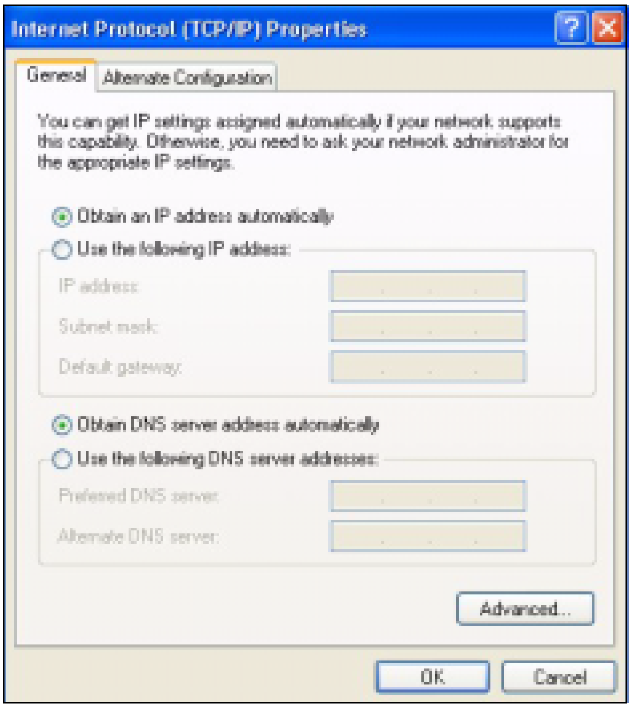
☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 87 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

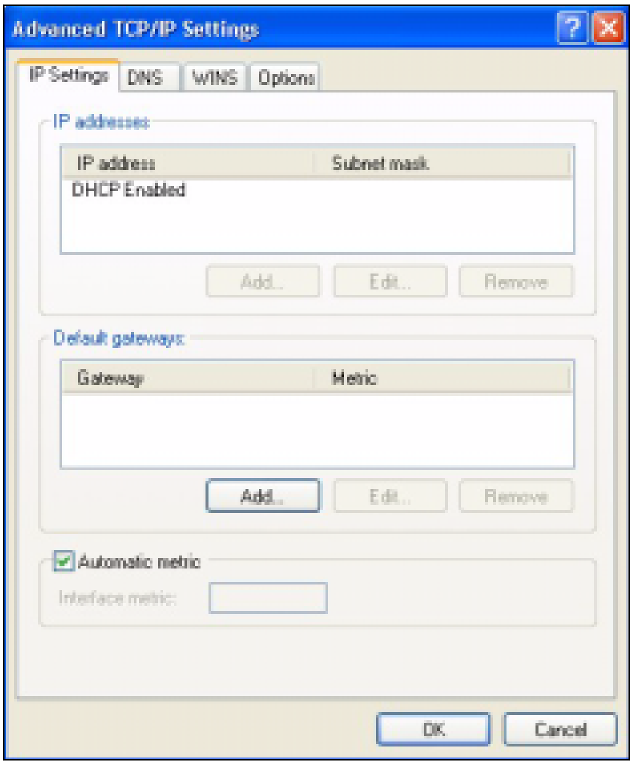
Alternate DNS server: . . .

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 88 Windows XP: Advanced TCP/IP Properties



IP address	Subnet mask
DHCP Enabled	

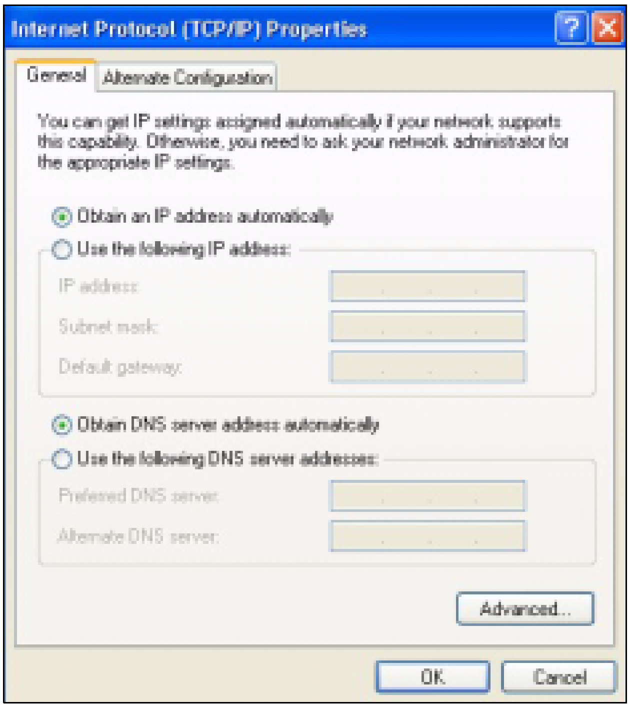
☑ Automatic metric

7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 89 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11Turn on your G-570S and restart your computer (if prompted).

Verifying Settings

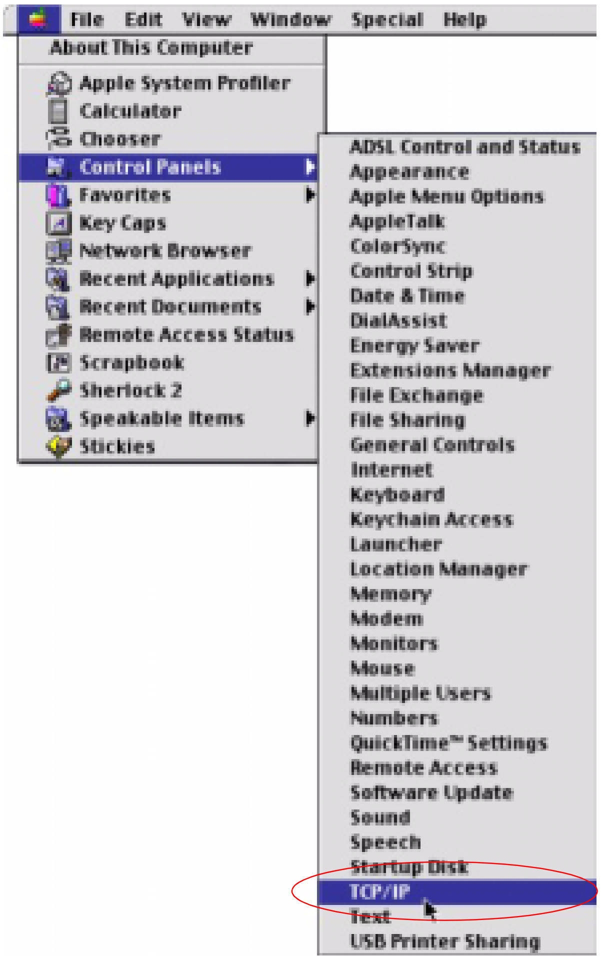
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

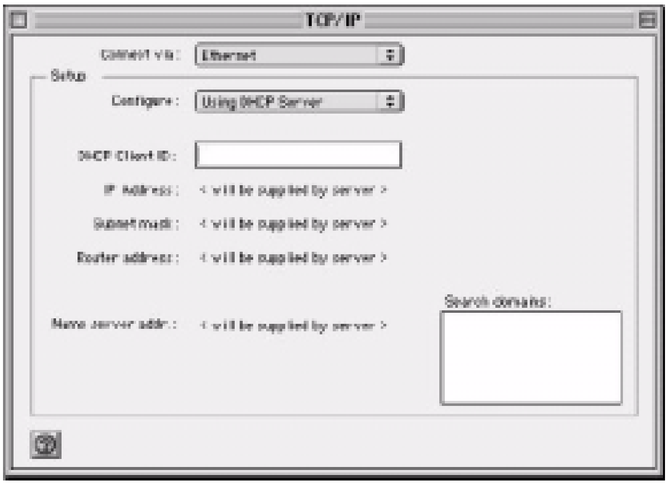
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 90 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 91 Macintosh OS 8/9: TCP/IP


TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your G-570S in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your G-570S and restart your computer (if prompted).

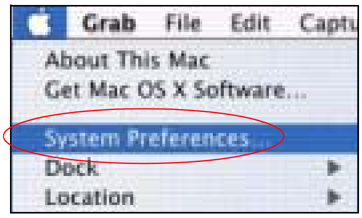
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 92 Macintosh OS X: Apple Menu

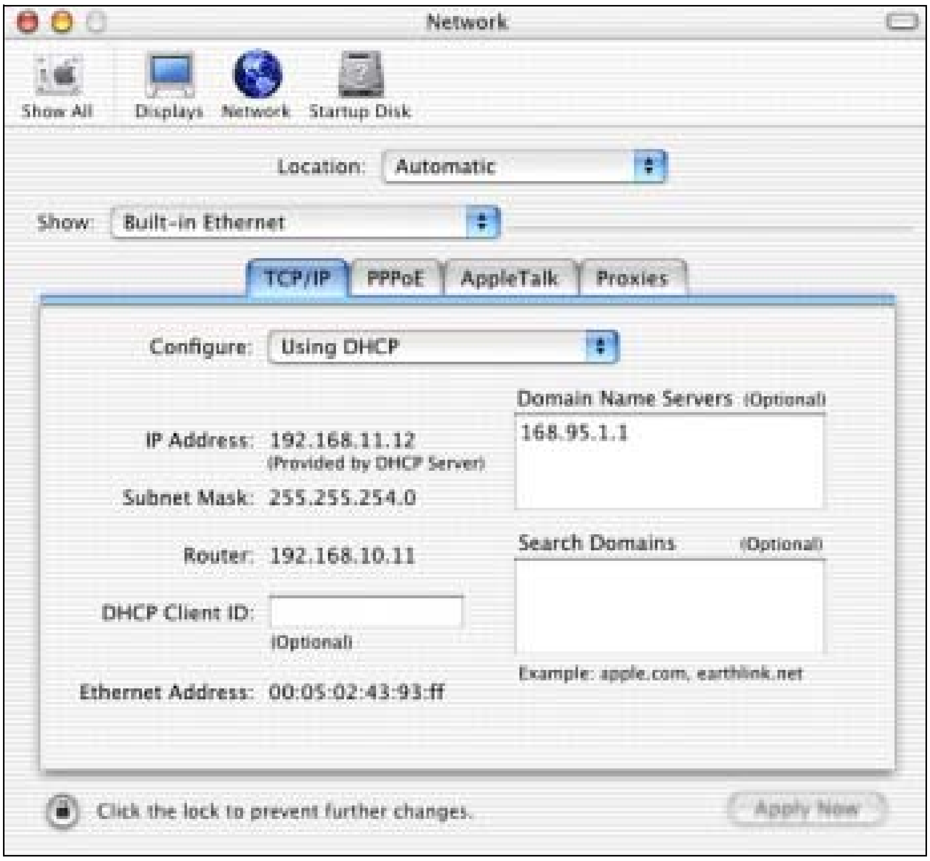


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 93 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your G-570S in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your G-570S and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer’s TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

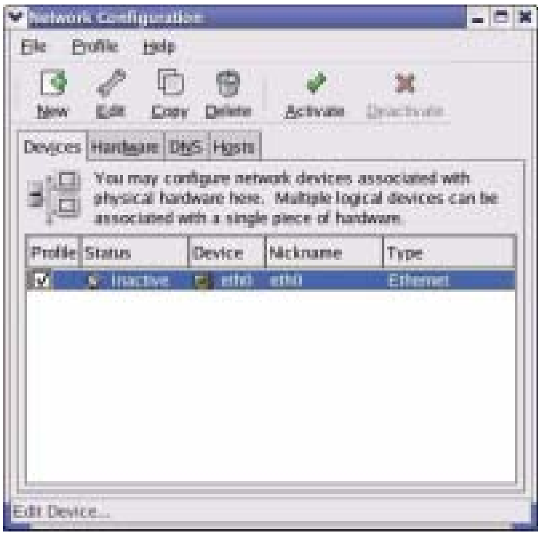
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 94 Red Hat 9.0: KDE: Network Configuration: Devices



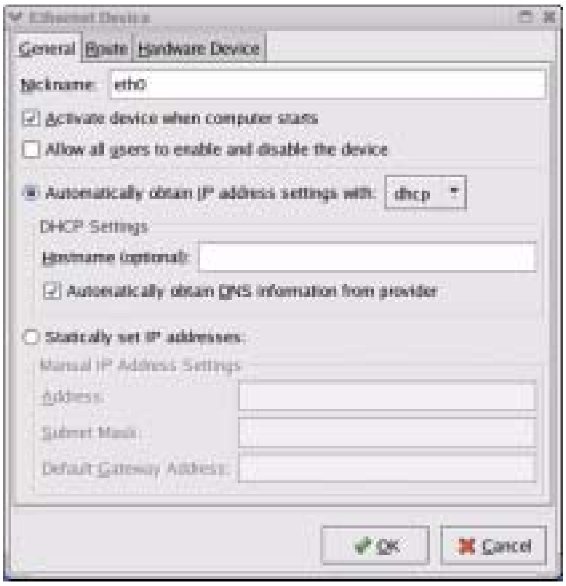
You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

Edit Device...

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 95 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

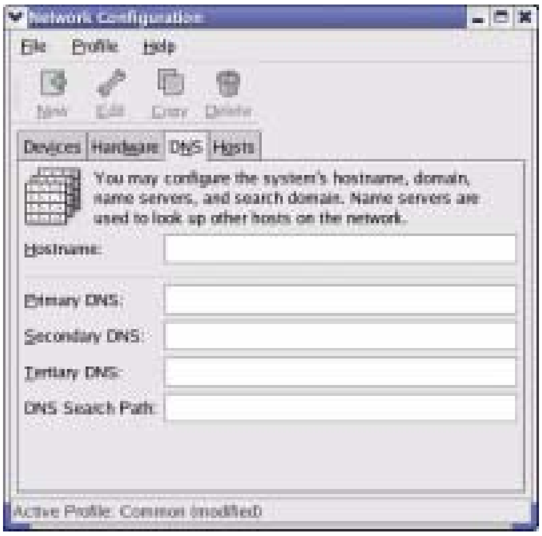
Default Gateway Address:

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 96   Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

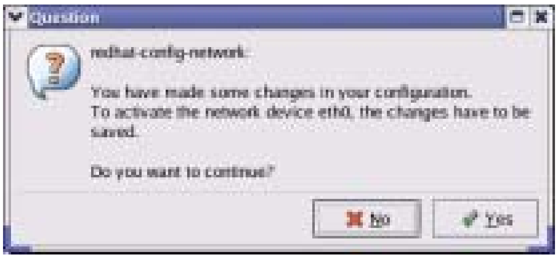
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

Figure 97   Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 98 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 99 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

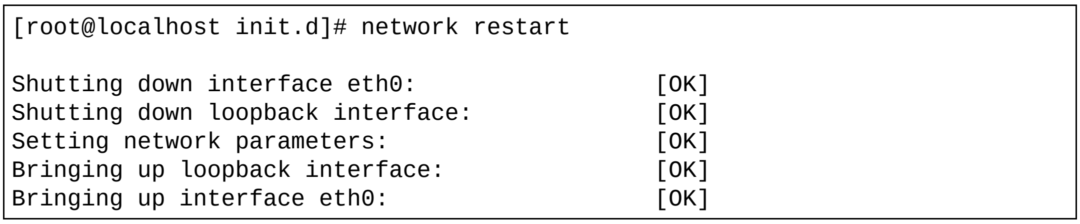
2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 100 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 101 Red Hat 9.0: Restart Ethernet Card



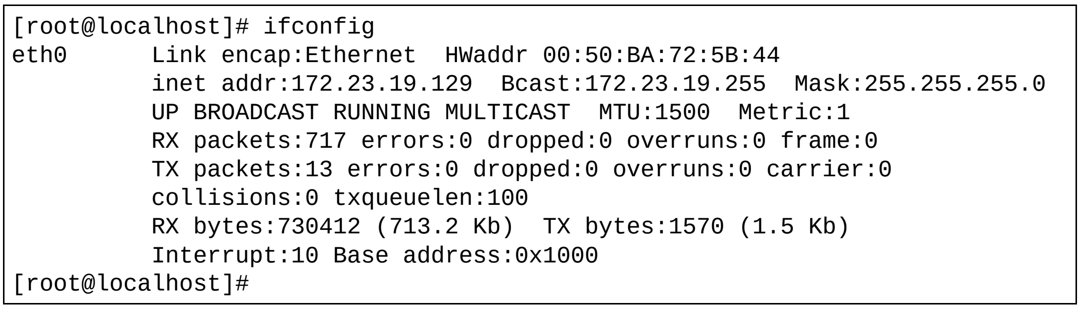
```
[root@localhost init.d]# network restart

Shutting down interface eth0:                    [OK]
Shutting down loopback interface:                [OK]
Setting network parameters:                      [OK]
Bringing up loopback interface:                  [OK]
Bringing up interface eth0:                      [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 102 Red Hat 9.0: Checking TCP/IP Properties



```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

APPENDIX C
Wireless LANs

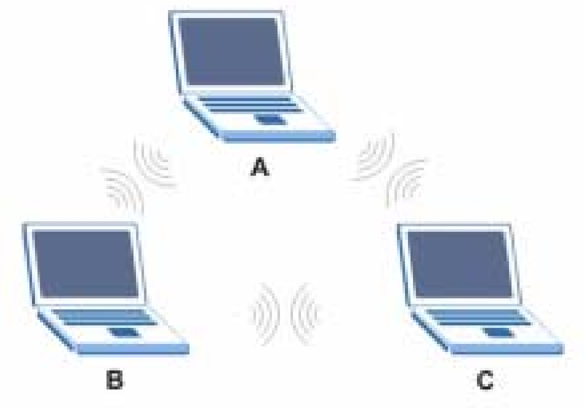
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 103 Peer-to-Peer Communication in an Ad-hoc Network

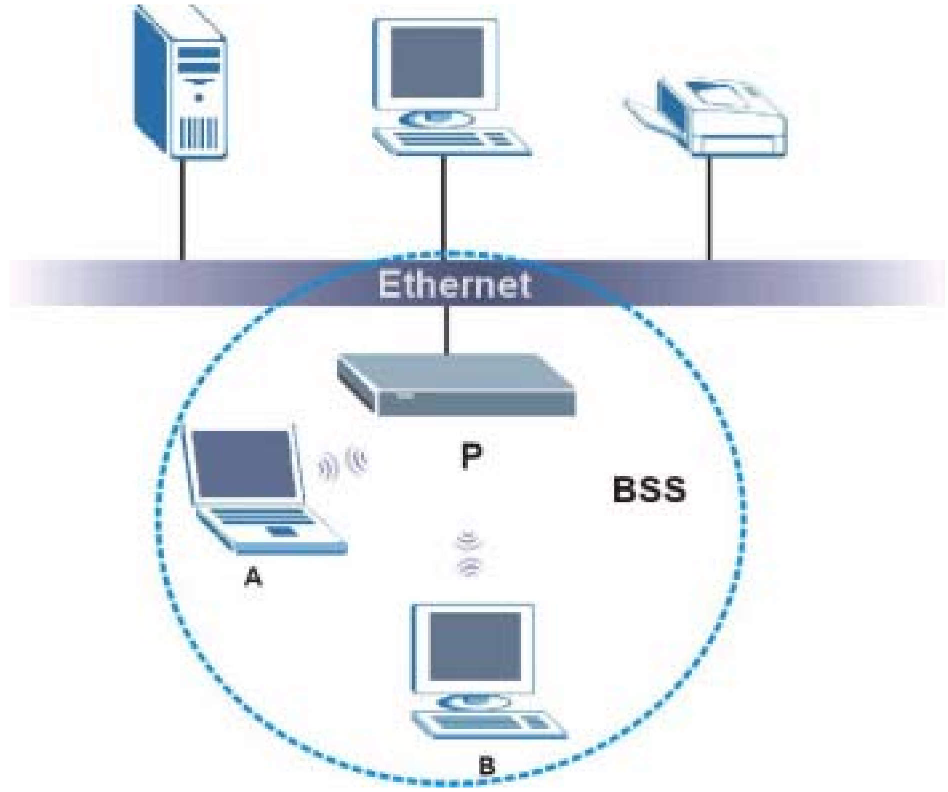


BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 104 Basic Service Set



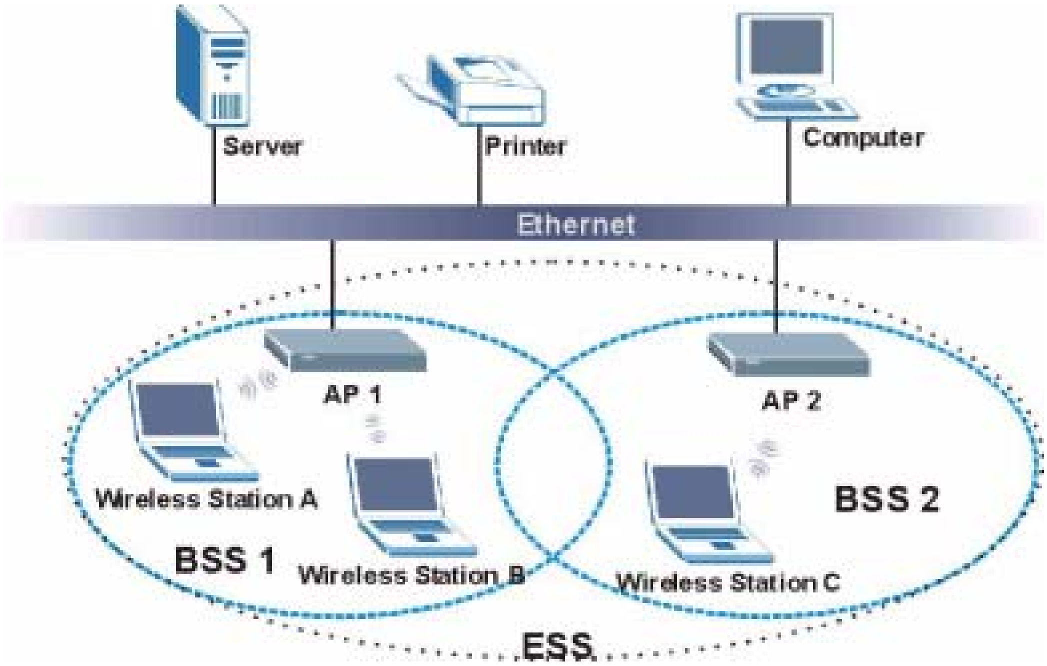
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 105 Infrastructure WLAN



Channel

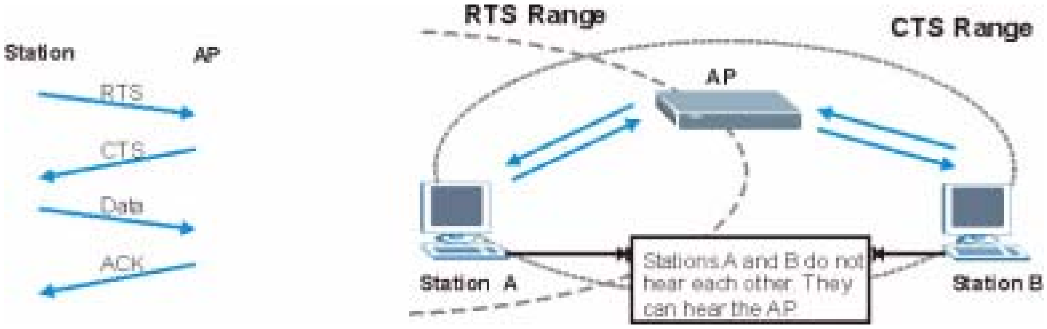
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 106 RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP

When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 37 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

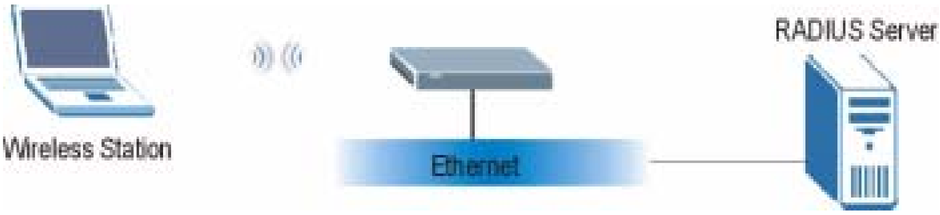
EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

Figure 107 EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

1 The wireless station sends a "start" message to the device.

2 The device sends a "request identity" message to the wireless station for identity information.

3 The wireless station replies with identity information, including username and password.

4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

Types of Authentication

This section discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

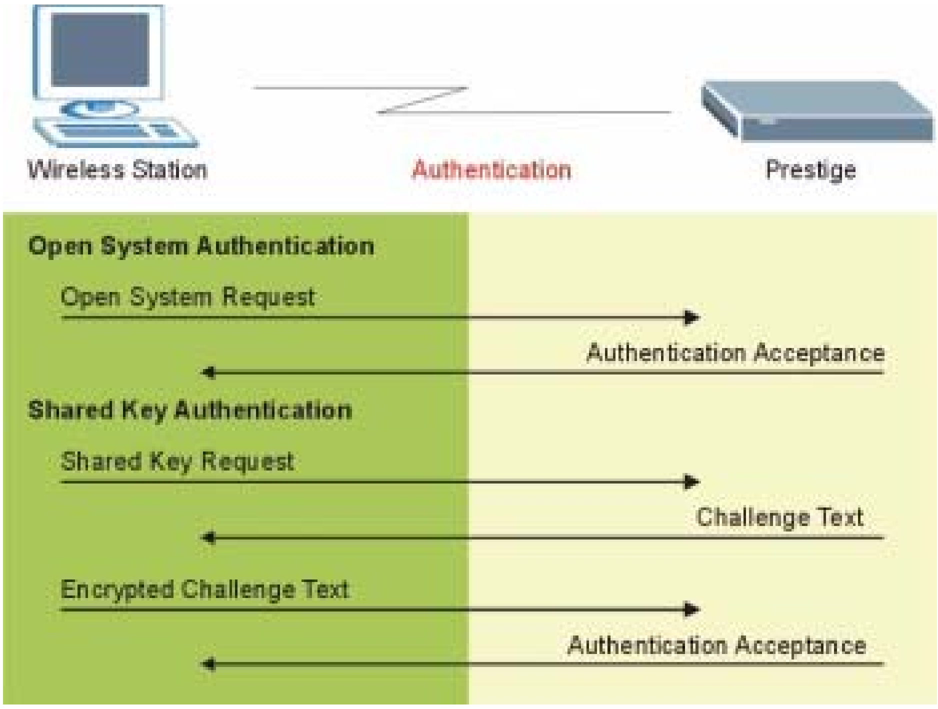
WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

WEP Authentication Steps

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.

Figure 108 WEP Authentication Steps



Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP’s default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP’s default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your device authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the device will accept either type of authentication request and the device will fall back to use open authentication if the shared key does not match.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 38 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA(2)

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decrypt data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

Roaming

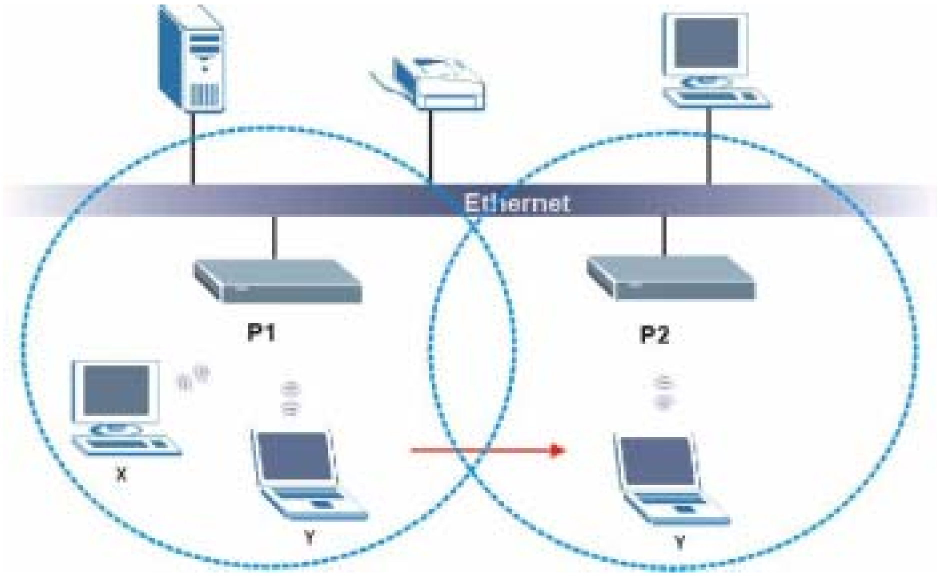
A wireless station is a device with an IEEE 802.11 mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point’s coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in Figure 109.

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

Figure 109 Roaming Example



The steps below describe the roaming process.

1 As wireless station **Y** moves from the coverage area of access point **P1** to that of access point

2 **P2**, it scans and uses the signal of access point **P2**.

3 Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.

4 Access point **P1** updates the new position of wireless station.

5 Wireless station **Y** sends a request to access point **P2** for re-authentication.

Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1 All the access points must be on the same subnet and configured with the same ESSID.

2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

3 The adjacent access points should use different radio channels when their coverage areas overlap.

4 All access points must use the same port number to relay roaming information.

5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

APPENDIX D
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Table 39 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class "C" network (8 host bits) can have 2^{8} –2 or 254 hosts.

A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Table 40 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Table 41 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

Table 42 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 43 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

Table 44 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 45 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 – 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Table 46 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 47 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 48 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 49 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 50 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class “C” subnet planning.

Table 51 Class C Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see Table 39 on page 151) available for subnetting.

The following table is a summary for class “B” subnet planning.

Table 52 Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Index