FT200 Series Wireless Access Point

Model FT213

User's Manual

Table of Content

Chapter 1: Introduction

This manual covers the installation and operation of the Comtec's FT213 Wireless Access Point. This Access Point provides a secure, affordable, and easy-to-use wireless LAN solution that combines flexibility with the enterprise-class features required by networking professionals.

This chapter gives an overview of the enterprises-class access point, as well as its key features. In addition, we detail about the hardware description, system requirement and basic installation.

Overview

FT213 access point distinguishes herself by one built-in mini-PCI card, providing wired and wireless two ports in a bigger infrastructure. Typically, VAP functionality allows a single network AP to behave as "8" number of virtual network APs. This does away with the limitation by the sheer number of Ethernet connections that need APs acting as a proxy. WMM prioritizes traffic demands from different applications and extends Wi-Fi's high quality end-user experience from data connectivity to voice, music, and video applications under a wide variety of environment.

This Access points serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

You can configure and monitor FT213 using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun. Use the instructions in this Guide to help you connect FT213, set it up, and configure it to bridge your different networks.

Key Features

FT213 is use-friendly and provides solid wireless and networking support. The following standards and conventions are supported:

- Standards Compliant. The Wireless Access Point complies with the IEEE 802.11a/b/g for Wireless LANs.
- WEP support. Support for WEP is included 64-bit, 128-bit, and 152-bit keys.
- DHCP Client Support. DHCP Server provides a dynamic IP address to PCs and other devices upon request. The FT213 can act as a client and obtain information from your DHPC server.
- RADIUS Accounting - Enable accounting on FT213 to send accounting data about wireless client devices to a RADIUS server on your network.
- SNMP Support. Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.
- Multiple operating modes:
  Access point
  Station Adapter
  Wireless Bridge.
  Wireless Repeater

Inter-building

- Repeater mode—Configure FT213 as a wireless repeater to extend the coverage area of your wireless network.
- VAPs
  Assign Multi-SSIDs on your access point (one SSID per VAP) to differentiate policies and services among users forming a wide variety of VLANs.
- QoS
  Use this feature to support quality of service for prioritizing traffic from the Ethernet to FT213. FT213 also supports the voice-prioritization schemes used by 802.11a/b/g wireless phones.
- Transmit Power Control
  Supports settable transmit power levels to adjust coverage cell size, ranging from full, half(50%), quarter(25%) eighth(12.5%) and min
- Atheros Super AG Mode: Super AG mode enables the transmission up to 108Mbps
- Multiple security settings per VLAN with up to 8 VLANs
  Security settings for multiple groups – so employees, guests and contractors now easily and securely share the same infrastructure
- Access Control.
  The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the to gain access to your LAN.
- Hidden Mode
  The SSID is not broadcast assuring only clients configured with the correct SSID can connect.

Preparation for Use

The Comtec's FT213 Wireless Access Point requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation and roaming.
The FT213 operates with Power over Ethernet (PoE) which requires the installation of a separate Power injector which "injects" DC current into the Cat5 cable.

The FT213 package includes the following items:

- The FT213 Wireless Access Point
- POE Power Injector
- AC Power Cord
- Mast Mounting Kit & Screw
- Documentation as PDF files (on CD-ROM)
- Quick installation guide

The FT213 can be mounted outdoor on a high post to achieve the best bridge result. If mounted outdoor, the outdoor protection kit must be used to prevent lightning damage.

Minimum System and Component Requirements

The FT213 is designed to be attached to the Mast at appropriate locations. To complete the configuration, you should have at least the following components:

- Access to at least one laptop or PC with an Ethernet card and cable that can be used to complete the initial configuration of the unit.

- A Web browser program (such as Microsoft Internet Explorer 6.0 or later, or Netscape 4.78 or later) installed on the PC or laptop you will be using to configure the Access Point.
- TCP/IP Protocol (usually comes installed on any Windows PC.)

Chapter 2: Basic Installation and Securities

This chapter explains how to place and connect the Comtec's Access Point. In addition, the security features are elaborated.
Note

You need to prepare these three things before you can establish a connection through your wireless access point.

- A location for the that conforms to the Observing Placement and Range Guidelines below.
- The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11a/b/g.

Operating Distance Tips

The range of your wireless connection is significantly determined by the physical placement of FT213.
To optimize the results, place your wireless access point:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones. • Away from large metal surfaces.
- Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11).

Default Factory Settings

We'll detail about FT213 default factory settings below. Factory Default Restore will enable you to restore these defaults.

FEATURE	FACTORY DEFAULT SETTINGS
User Name (case sensitive)	admin
Password (case sensitive)	password
Access Point Name	APxxxxxx(xxxxxx represents the last 6 digits of MAC address)
Country / Region	United States
Router Mode	Bridge
IP Type	static IP

IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Operating Mode	Access Point
Wireless Mode	802.11a
Channel / Frequency	52 / 5.260GHz

Getting To Know Wireless Security Options

Comtec wants to make wireless networking as safe and easy for you as possible. The current generation of products provides several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take as shown in this User's Manual. (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

To ensure network security, steps one through four should be followed, at least. Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier).

Security Options

There are several ways you can enhance the security of your wireless network:

- Restrict Access Based on MAC address. You can restrict access to only trusted clients so that unknown clients cannot wirelessly connect to the FT213. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- Use WEP. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- Use WPA or WPA-PSK. Wi-Fi Protected Access (WPA) data encryption provides data WPA makes it virtually impossible to compromise.
- Enable Wireless Security Separator

The associated wireless clients will not be able to communicate with each other if this feature is enabled. The default setting is Disable.

Installing FT213 Access Point

Before installing, you should make sure that Ethernet network is perfectly working. You will be connecting the FT213 to the Ethernet network so that computers with 10/100 Fast Ethernet adapters will communicate computers on the Ethernet.

SETUP THE ACCESS POINT Tip

Before mounting the FT213 in a high location, first set up and test the FT213 to verify wired network connectivity.

a. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.

b. Configure the computer with a static IP address of 192.168.1.x (x cannot be 1)and 255.255.255.0 for the Subnet Mask.

c. Connect an Ethernet cable from the FT213 to the computer.

d. Turn on your computer, connect the power adapter to the FT213

CONFIGURE LAN AND WIRELESS ACCESS

Configure the Ethernet port for LAN access

- Connect to the FT213 by opening your browser and entering http://192.168.1.1 in the address field. A login window like the one shown below opens:

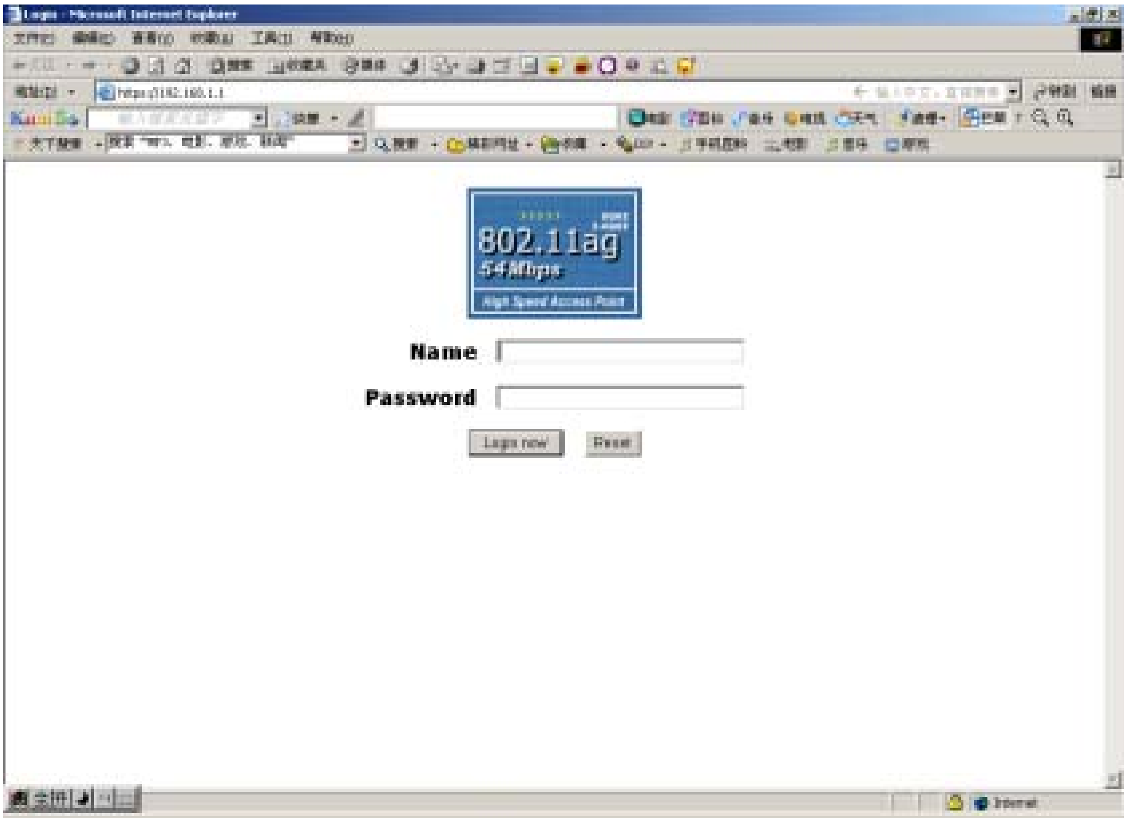
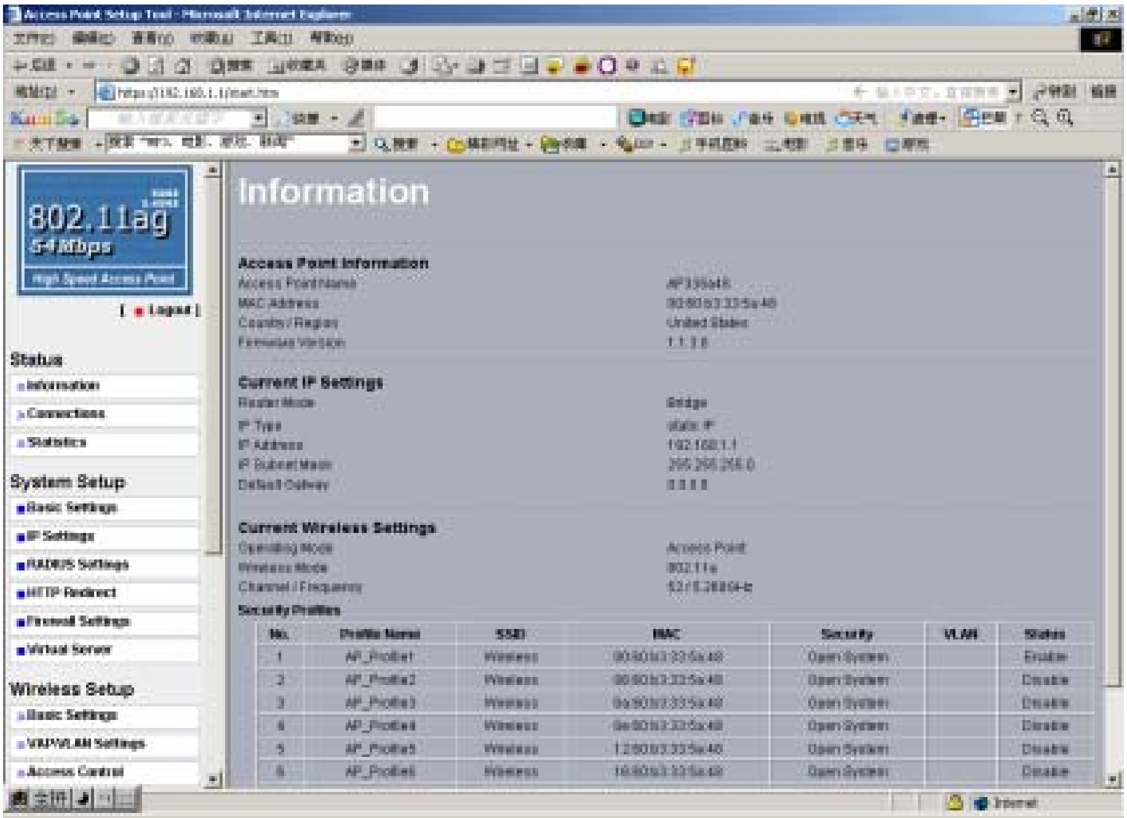


Figure: 2-1 login window

When prompted, please enter **admin** for Name and password for **password**, Clicking

Login now, it will navigate you into FT213’s homepage-----General Information will be shown below.



Information

Access Point Information

Access Point Name	AP335a40
MAC Address	00:90:b3:33:5a:40
Country / Region	United States
Firmware Version	1.1.3.8

Current IP Settings

Router Mode	Bridge
IP Type	static IP
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

Current Wireless Settings

Operating Mode	Access Point
Wireless Mode	802.11a
Channel / Frequency	52 / 5.26GHz

Security Profiles

No.	Profile Name	SSID	MAC	Security	VLAN	Status
1	AP_Profile1	Wireless	00:90:b3:33:5a:40	Open System		Enable
2	AP_Profile2	Wireless	06:90:b3:33:5a:40	Open System		Disable
3	AP_Profile3	Wireless	0a:90:b3:33:5a:40	Open System		Disable
4	AP_Profile4	Wireless	0e:90:b3:33:5a:40	Open System		Disable
5	AP_Profile5	Wireless	12:90:b3:33:5a:40	Open System		Disable
6	AP_Profile6	Wireless	16:90:b3:33:5a:40	Open System		Disable

Figure: 2-2 general information

Deploy the FT213 Access Point

a. Disconnect the FT213 and position it where you will deploy it. The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.

b. Lift the antenna on either side so that they are vertical.

Note: Consult the antenna positioning and wireless mode configuration information in the Advanced Configuration chapter of the Reference Manual.

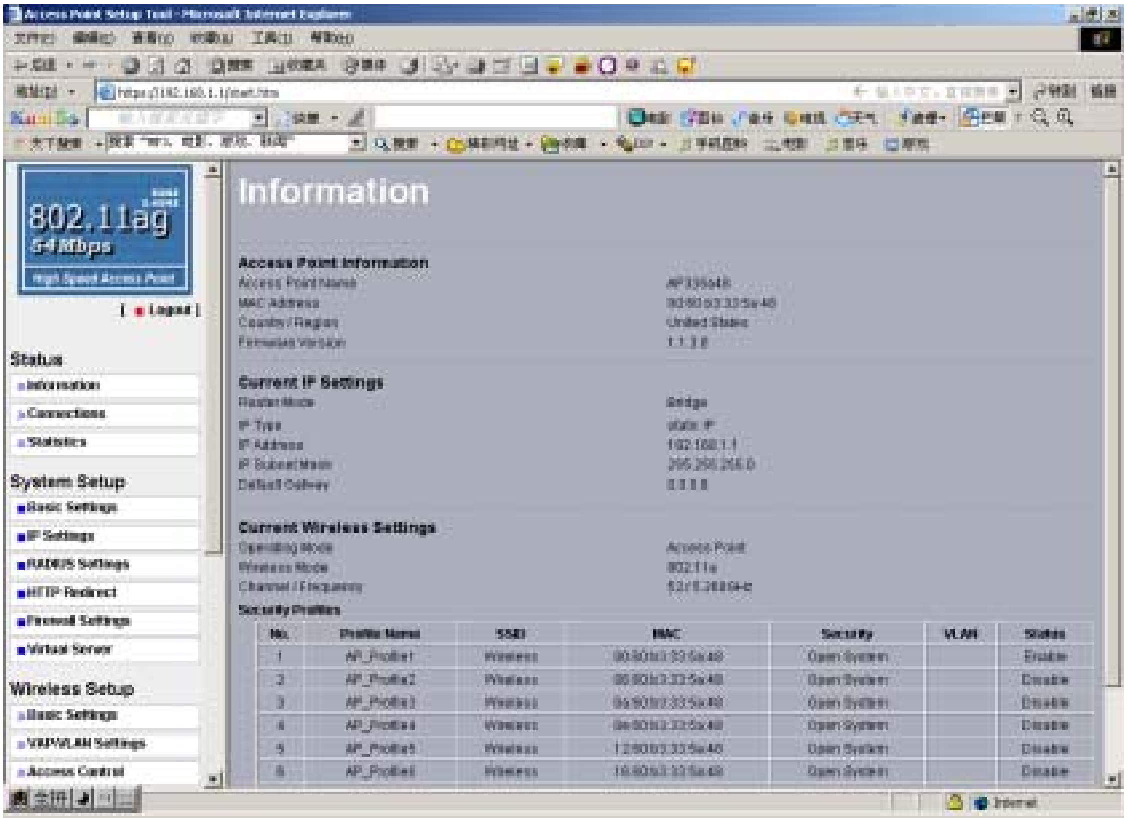
c. Connect an Ethernet cable from your FT213 Access Point to a LAN port on your router, switch, or hub.

d. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet.

Chapter 3: General Information

General information gives you a basic concept of the FT213 Access Point.

Information



Information

Access Point Information

Access Point Name	AP335a48
MAC Address	00:80:b3:33:5a:48
Country / Region	United States
Firmware Version	1.1.3.8

Current IP Settings

Router Mode	Bridge
IP Type	static IP
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

Current Wireless Settings

Operating Mode	Access Point
Wireless Mode	802.11a
Channel / Frequency	52 / 5.26GHz

Security Profiles

No.	Profile Name	SSID	MAC	Security	VLAN	Status
1	AP_Profile1	Wireless	00:80:b3:33:5a:48	Open System		Enable
2	AP_Profile2	Wireless	06:80:b3:33:5a:48	Open System		Disable
3	AP_Profile3	Wireless	0a:80:b3:33:5a:48	Open System		Disable
4	AP_Profile4	Wireless	0e:80:b3:33:5a:48	Open System		Disable
5	AP_Profile5	Wireless	12:80:b3:33:5a:48	Open System		Disable
6	AP_Profile6	Wireless	16:80:b3:33:5a:48	Open System		Disable

Figure: 3-1 general information

We'll elaborate the information from the FT213's homepage

Access Point Name: You may assign any device name to FT213. This name is only used by FT213 administrator for identification purposes. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. The default name is APxxxxxx..

MAC Address: Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.

Country/Region: This field identifies the region where the FT213 can be used. It may not be legal to operate the wireless features of the wireless access point in a region other than one of those identified in this field. The default country is the United States.

Firmware Version: Firmware is stored in a flash memory and can be upgraded easily, using your Web browser, and can be upgraded via ftp server or ftp server. IP Type: By default, the FT213 is configured as static IP Address.

IP Address: The IP address must be unique to your network. The default IP address is 192.168.1.1

Note

To associate FT213 to your PC, make sure the PC IP address need to be matched the AP. For instance, the FT213 is 192.168.1.1, and your PC IP should be 192.168.1. X.

Subnet Mask: The Subnet Mask must be the same as that set on the LAN that your Access Point is connected to. The default is 255.255.255.0.

Operating Mode: provides five modes, Access Point, Station, bridge, repeater and inter-building.

Access Point: Act as a standard 802.11a/b/g. The default mode is Access Point.

Station: Perform as a client station associated to other APs. Be sure that they share the same SSID when connected.

Bridge: The FT213 acts as a bridge connecting APs. Two bridge modes are available below.

Point-to-Multi-Point Bridge: Select this only if this is the "Master" for a group of bridges. The other bridge must use this MAC address. They then send all traffic to this "Master", rather than communicate directly with each other. WEP should be used to protect this traffic.

Wireless Repeater: In this mode, the FT213 can communicate with another wireless station or wireless bridge. You can enter the MAC address of both adjacent repeaters in the fields provided to communicate with other wireless bridge or use SSID to communicate with other wireless station. WEP should be used to protect this communication.

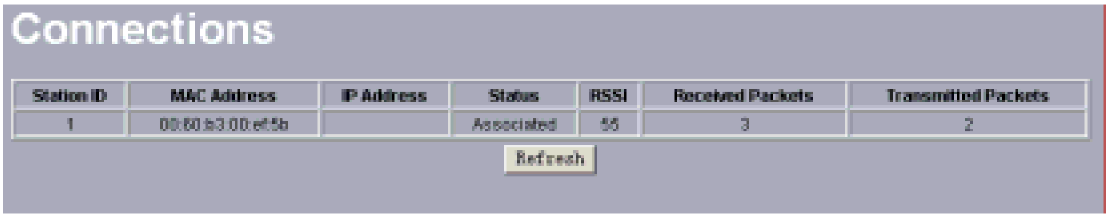
Wireless Mode: Select the desired wireless operating mode. The default mode is 802.11a.

Channel: This field identifies which operating frequency will be used.

Security Profiles: This provides a list of virtual APs derived from FT213 Virtual AP, spelling out profile name, SSID, MAC, security, and status.

Connection

Under the Information heading, click the connection link to view the connection status shown below.



Connections

Station ID	MAC Address	IP Address	Status	RSSI	Received Packets	Transmitted Packets
1	00:60:b3:00:ef:5b		Associated	55	3	2

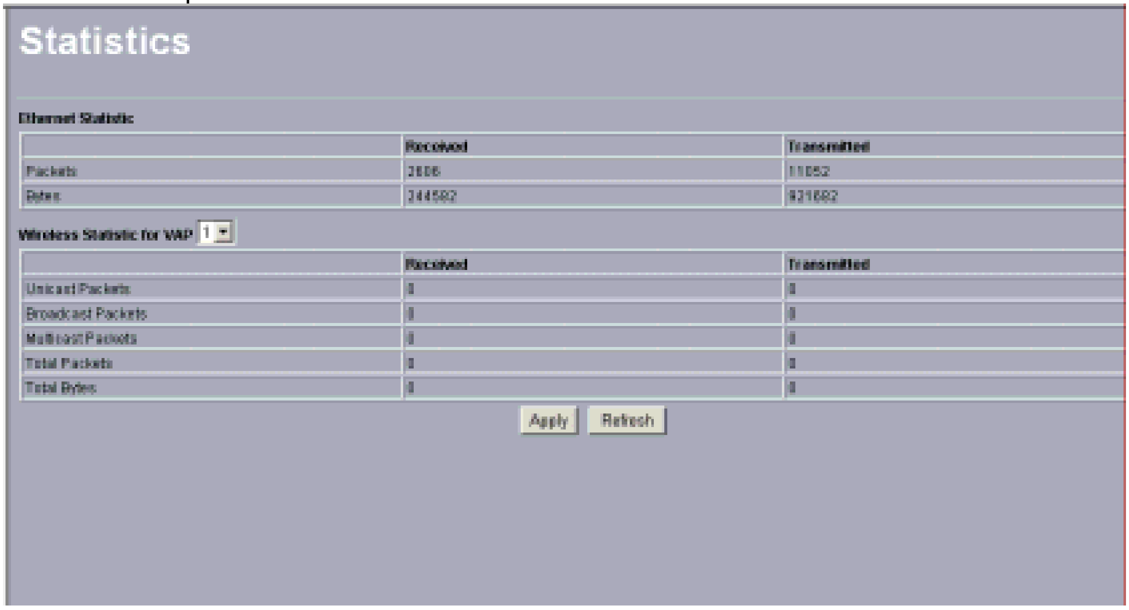
Figure: 3-2 connection status

Note

If the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices.

Statistics

The statistics provide various LAN and WAN statistics.



Statistics

Ethernet Statistic

	Received	Transmitted
Packets	2806	11052
Bytes	344582	921682

Wireless Statistic for VAP 1

	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	0
Multicast Packets	0	0
Total Packets	0	0
Total Bytes	0	0

Figure: 3-3 statistics

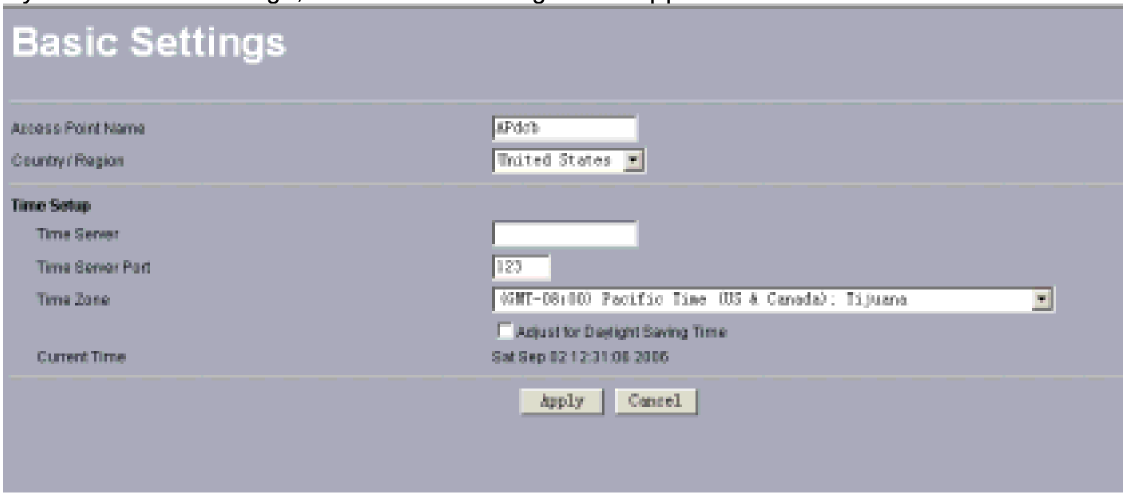
Field		**Description**
Wired Ethernet	Packets	The number of packets sent since the was restarted.
	Bytes	The number of bytes sent since the was restarted.
Wireless	Unicast Packets	The Unicast packets sent since the was restarted.
	Broadcast Packets	The Broadcast packets sent since the was restarted.
	Multicast Packets	The Multicast packets sent since the was restarted.
	Total Packets	The Wireless packets sent since the was restarted.
	Total Bytes	The Wireless bytes sent since the was restarted.

Chapter 4: Copious Functionalities

The versatile FT213 access point provides various, applicable functions.

Time Server

By click Basic Settings, the “Basic Settings” will appear shown below.



Basic Settings

Access Point Name: APdcb

Country / Region: United States

Time Setup

Time Server:

Time Server Port: 123

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

□ Adjust for Daylight Saving Time

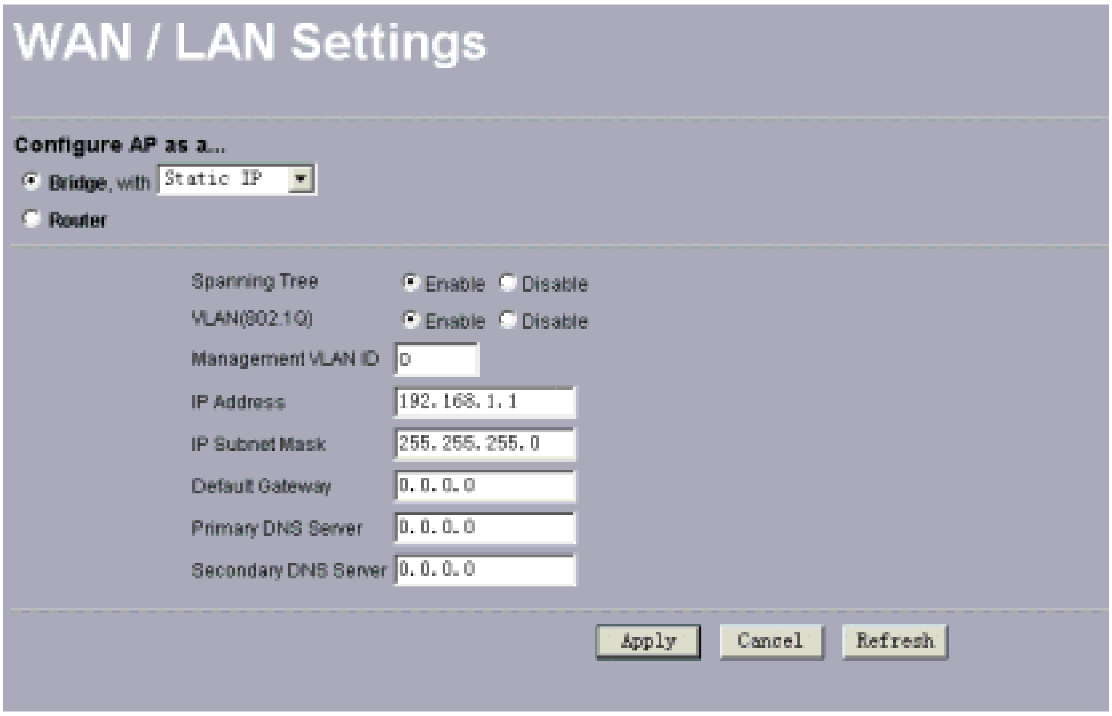
Current Time: Sat Sep 02 12:31:08 2006

Figure: 4-1 Basic settings

The FT213 allows you to synchronize the time between your network and time server by using NTP Time Server.
Time Sever provides correct and current time in any world time zone, country or major city. Accurate adjustments for Daylight Saving Time (or Summer Time) are made according to each location's rules and laws.
Time Server Port: This field identifies the time server port like 123.
Time Zone: Select the time zone location for your setting.
Current Time: This field identifies the current time in your specific time Zone.

Bridge / Router Mode

From the system setup, click IP Settings, you’ll be navigated into the WAN/LAN Settings.



WAN / LAN Settings

Configure AP as a...

● Bridge, with Static IP

○ Router

Spanning Tree	● Enable ○ Disable
VLAN(802.1Q)	● Enable ○ Disable
Management VLAN ID	0
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Figure: 4-2 WAN/LAN settings

FT213 can be figured as bridge mode and router mode.

Bridge Mode

Under Bridge Mode, the FT213 will act as a pass-through bridging your network, by associating with various devices. This can extend your radius of your network.

Spanning Tree: Enabling spanning tree can prevent undesirable loops in the network, ensuring a smooth running network. By default, the function is enabled.

Router Mode

Under Router Mode, the FT213 has two ports, WAN port and LAN ports.

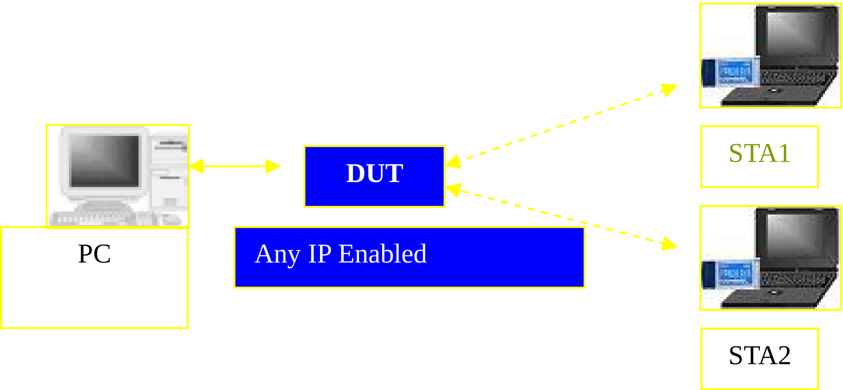
If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu. These settings are only required if the Refresh" is chosen. Remember to click Apply to save your changes.

Any IP

If IP address has slipped your mind, any IP functionality can relieve your anxiety. Enabling any IP, you'll feel free to enter IP Address, IP Subnet Mask and Gateway, enjoying internet surf.

Please refer to the diagram below.

Take the steps to activate the functionality.

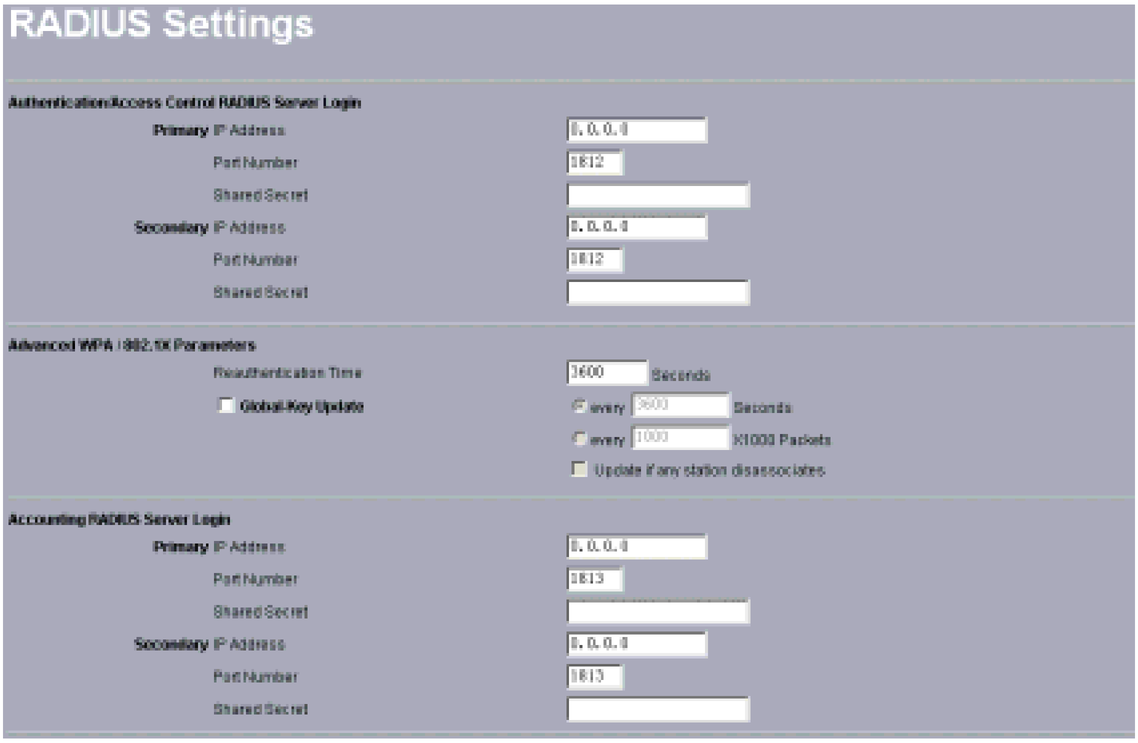


Configure the FT213 as router mode.
Make sure your station connected to the AP.
Set correct IP parameters for the AP.
Enable any IP

Understanding RADIUS Settings

RADIUS is a server for remote user authentication and accounting. It can be used on any network that needs a centralized authentication and/or accounting service for its workstations.

From the system Setup, click Radius Settings, the RADIUS Settings will display as below.



RADIUS Settings

Authentication/Access Control RADIUS Server Login

Primary IP Address	0. 0. 0. 0
Port Number	1812
Shared Secret	
Secondary IP Address	0. 0. 0. 0
Port Number	1812
Shared Secret	

Advanced WPA / 802.1X Parameters

Reauthentication Time	3600 Seconds
□ **Global-Key Update**	● every 3600 Seconds
	○ every 1000 X1000 Packets
	□ Update if any station disassociates

Accounting RADIUS Server Login

Primary IP Address	0. 0. 0. 0
Port Number	1813
Shared Secret	
Secondary IP Address	0. 0. 0. 0
Port Number	1813
Shared Secret	

Figure: 4-3 Radius settings

You will also have to fill in the following Radius server settings:

- Primary Radius Server IP Address

This field is required. Enter the IP address of the Radius Server on your LAN or WAN..

- Secondary Radius Server IP Address

  This field is optional. Enter the IP address of the Secondary Radius Server on your LAN.
- Radius Port

  Enter the port number used for connections to the Radius Server.
- Radius Shared Key

  Enter the desired value for the Radius shared key. This key enables the client to log in to the Radius server and must match the value used on the Radius server.
- Radius Accounting Option

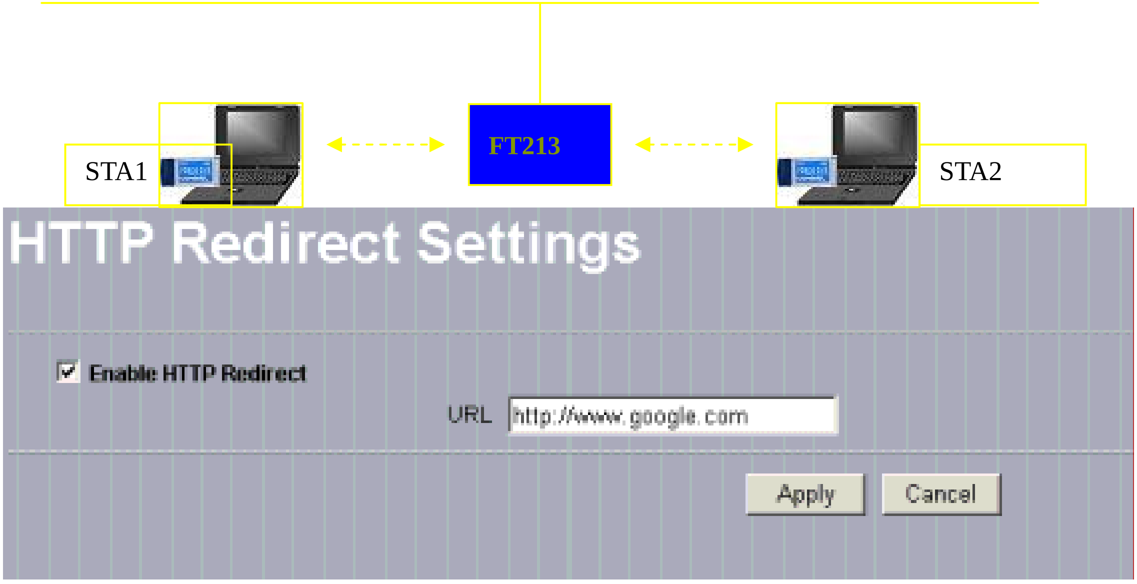
  The Radius Accounting option can be enabled so that you can track various information like who connected to the network, when they connected, how long they were connected, how much network traffic they generated, and so on.

HTTP Redirect

Currently market campaign has a stake in the future of your company, so that plugging your products on website is a basic step for your goods.

The FT213 access point has insight into your need. Enabling HTTP Redircet, you can enter the company website (for example, http://www.google.com). It is your desired web that first appear when someone is surfing on internet, via a station connected to your AP for internet surf.

The following is the HTTP Redirect Settings.



HTTP Redirect Settings

☑ Enable HTTP Redirect

URL http://www.google.com

Figure: 4-4 HTTP Redirect settings

URL

Enter your desired website in this field. Be sure to click “Apply” to save the configuration.

Note

Be sure to your AP connected to the internet when using HTTP Redirect.

Firewall Management

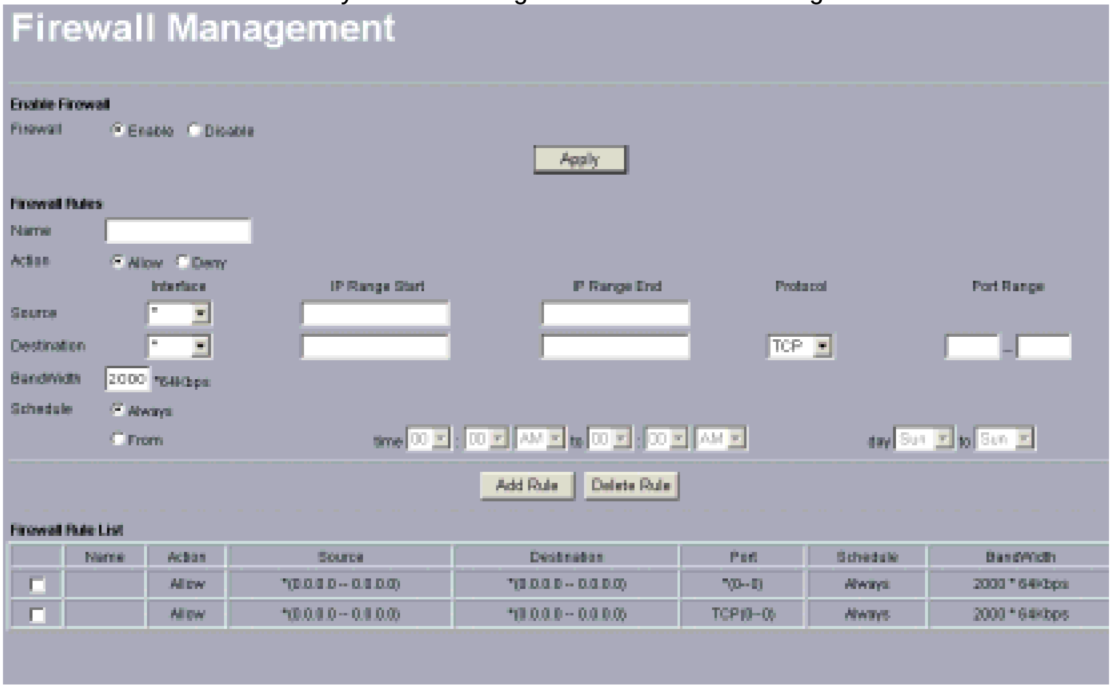
Today's companies rely on highly networked, secure computing environments to efficiently and safely conduct business. Firewalls are a key component of any secure network. Firewalls are configured to allow "desired" traffic in and to keep "undesired" traffic out.

The FT213 access point is also qualified for firewall management.

Please see the diagram below.

Acting as a firewall, the AP will filter your undesired data and protocols, only delivering the "wanted" for your PC.

Click the firewall link and you'll be navigated to Firewall Management interface.



Firewall Management

Enable Firewall

Firewall ● Enable ○ Disable

Apply

Firewall Rules

Name

Action ● Allow ○ Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	*				
Destination	*			TCP	–

BandWidth 2000 *64Kbps

Schedule ● Always

○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Add Rule Delete Rule

Firewall Rule List

	Name	Action	Source	Destination	Port	Schedule	BandWidth
□		Allow	*(0.0.0.0 -- 0.0.0.0)	*(0.0.0.0 -- 0.0.0.0)	*(0--0)	Always	2000 * 64Kbps
□		Allow	*(0.0.0.0 -- 0.0.0.0)	*(0.0.0.0 -- 0.0.0.0)	TCP(0--0)	Always	2000 * 64Kbps

Figure: 4-5 firewall management

Before applying the firewall management, you need enable firewall.

Here we'll discuss Firewall.

- Name
  Enter your desired firewall rule name in this field.
- Allow
  This field identifies which packets have IP addresses specified by you, are allowed to transmit at your LAN.
- Deny
  This field identifies which packets have IP addresses specified by you, are banned to transmit at your LAN.
- Interface
  This is optional, WAN or LAN.
- Destination
  This specifies where packets are bound for.
- IP Range Start

This specifies the starting-point of your specific IP addresses.

- IP Range End
  This specifies the ending-point of your specific IP addresses.
- Protocol
  This is optional, TCP, DCP, ICMP or *. Select which protocol you want to perform "Allow" or "Deny".

Note

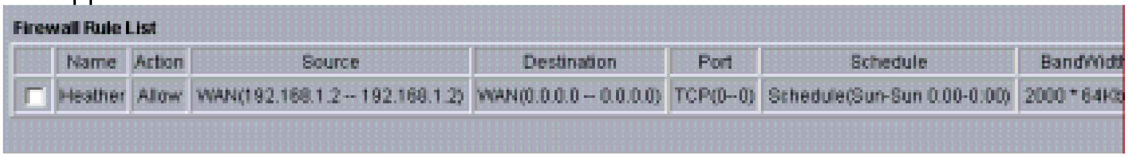
* indicates you restrict no protocol to perform "Allow" or "Deny".

- Port Range
  This specifies your IP port range.

Schedule

You can set time when your AP performs firewall management, by enabling "from". Alternatively, if you desire your AP to perform firewall management for a long time, please enable "always".

When completing all firewall rules configuration, please click Add Rule. Firewall Rule List will appear below.



Firewall Rule List

	Name	Action	Source	Destination	Port	Schedule	BandWidt
□	Heather	Allow	WAN(192.168.1.2 -- 192.168.1.2)	WAN(0.0.0.0 -- 0.0.0.0)	TCP(0--0)	Schedule(Sun-Sun 0:00-0:00)	2000 * 64K

Figure: 4-6 FT213 firewall list

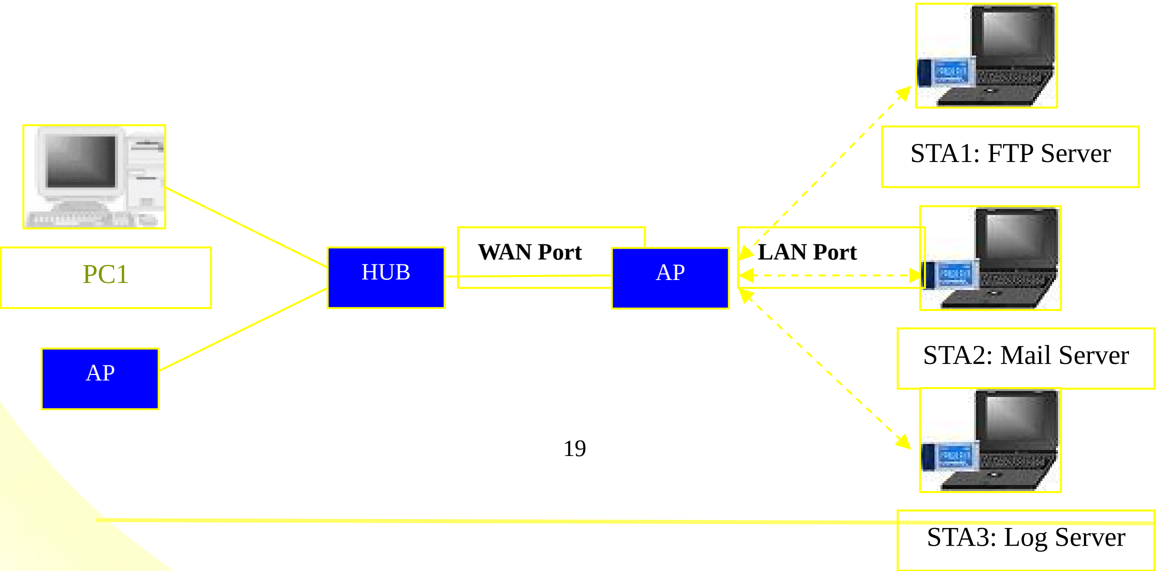
Virtual Server

Note

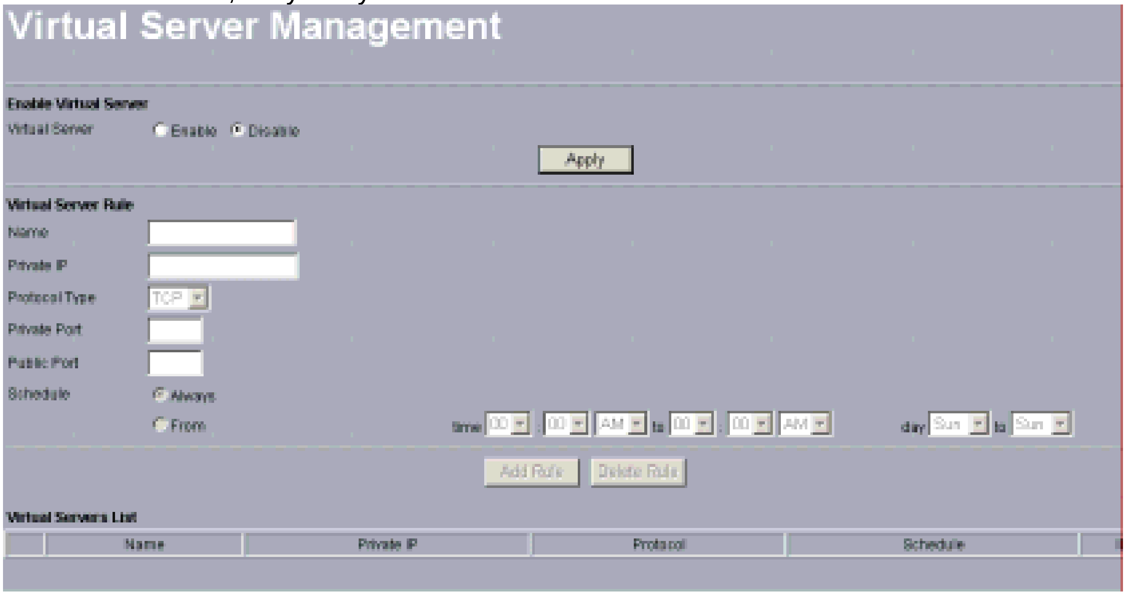
Virtual server can be enabled only under router mode.

The FT213 access point distinguishes by acting as a virtual server. This most cost-effective server virtualization technology is engineered for heterogeneous network. Please refer to the following diagram.

Under router mode, designed for the virtual server, the AP is wirelessly coupled to FTP server, mail server and log server on LAN port; on WAN port, the AP is coupled to PC.



The AP is the virtual server, so that you have access to download files, enjoy e-mails or undertake others, only via your PC.



Virtual Server Management

Enable Virtual Server

Virtual Server ○ Enable ● Disable

Virtual Server Rule

Name

Private IP

Protocol Type TCP

Private Port

Public Port

Schedule ● Always

○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Virtual Servers List

	Name	Private IP	Protocol	Schedule

Figure: 4-7 virtual server management

We'll discuss virtual elements below.

•Name

Enter the virtual server's name in this field.

•Private IP

This specifies the IP Address at your LAN.

•Protocol Type

This field is optional. Select TCP or UDP.

•Private Port

This specifies your LAN port.

•Public Port

This specifies your WAN port.

Schedule

You can set time-limit when your AP acts as a virtual server, by enabling "from". Alternatively, if you desire your AP to act as a virtual server for a long time, please enable "always".

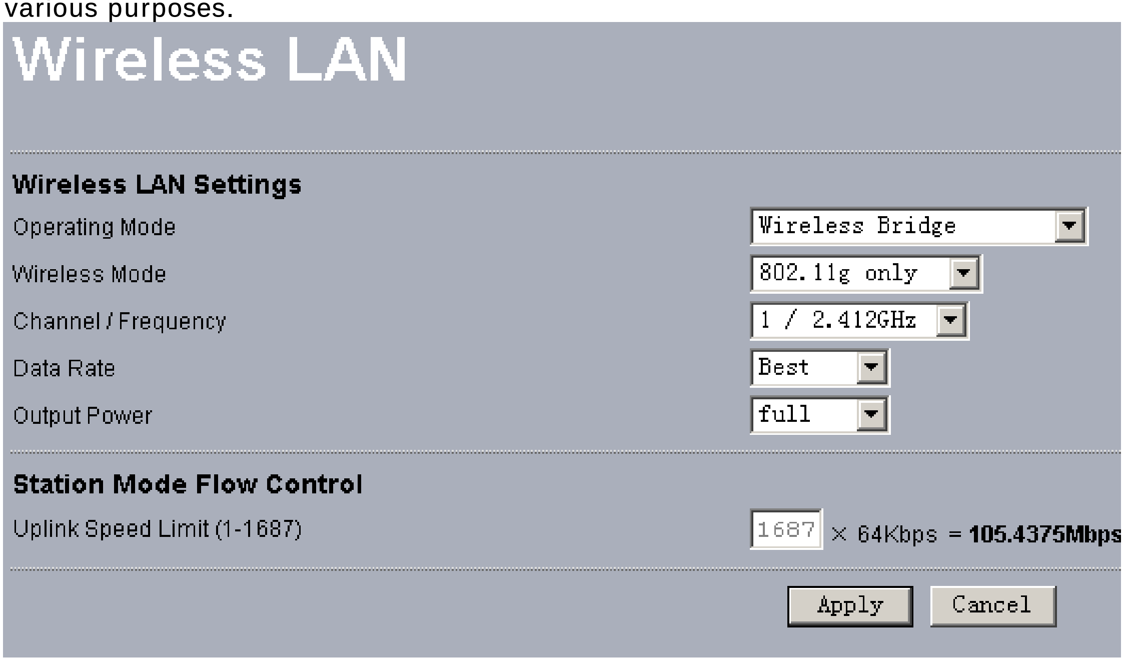
When completing configuration of your virtual server, please click "Add Rule" to save the setting.

•Virtual Server List

This provides you with the detailed list of virtual servers.

Chapter 5: Wireless Setup

This chapter focuses on the FT213 access point's powerful wireless function.
Basic Settings
The versatile FT213 access point proves adequate to five operating modes for your various purposes.



Wireless LAN

Wireless LAN Settings

Operating Mode: Wireless Bridge

Wireless Mode: 802.11g only

Channel / Frequency: 1 / 2.412GHz

Data Rate: Best

Output Power: full

Station Mode Flow Control

Uplink Speed Limit (1-1687): 1687 × 64Kbps = 105.4375Mbps

Figure: 5-1

Operating Mode

FT213 is capable of five operating modes, access point, station adapter, wireless bridge, wireless repeater, and wireless inter-building.

•Access Point
Any 802.11a/b/g wireless station can communicate with it by correct SSID.

•Wireless bridge
In this mode, the FT213 only communicates with another bridge-mode wireless station. You must enter the MAC address (physical address) of the other bridge-mode wireless station in the field provided. WEP should be used to protect this communication.

•Point to Multi-Point Bridge
Select this only if this FT213 is the "Master" for a group of bridge-mode wireless stations. The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using this FT213 MAC address. They then send all traffic to this "Master", rather than communicate directly with each other. WEP should be used to protect this traffic.

• Wireless Repeater.
In this half-duplex mode, the FT213 can communicate with another wireless bridge and wireless station. You must enter the MAC address of both adjacent wireless bridges in the fields provided. WEP should be used to protect this communication.

•Inter-building
This is Comtec own brand of WDS mode. Under this mode, FT213 will automatically connect XI-1500, without manually entering MAC address for each other.

•SSID

The SSID is the unique name shared among all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure this setting is the same for all devices in your wireless network. The default SSID name is wireless.

•BSSID

A group of Wireless Stations and a single access point, all using the same ID (SSID), form a Basic Service Set.

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some access points allow connections from wireless stations which have their SSID set to “any” or whose SSID is blank (null).

•Wireless Mode

Select the desired wireless operating mode. The options are:

11a only – Only 802.11a wireless stations can be used.

Auto (11g/b) – Both 802.11g and 802.11b wireless stations can be used.

11g only - Only 802.11g wireless stations can be used.

11b only - All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.

• Channel. This field identifies which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems or setting up the FT213 near another access point.

• Data Rate. Shows the available transmit data rate of the wireless network. The default is Best.

• Output Power. Set the transmit signal strength of FT213. The options are full, half, quarter, eighth, and min. Decrease the transmit power if more than one AP is collocated using the same channel frequency. The default is Full.

Station Mode Flow Control

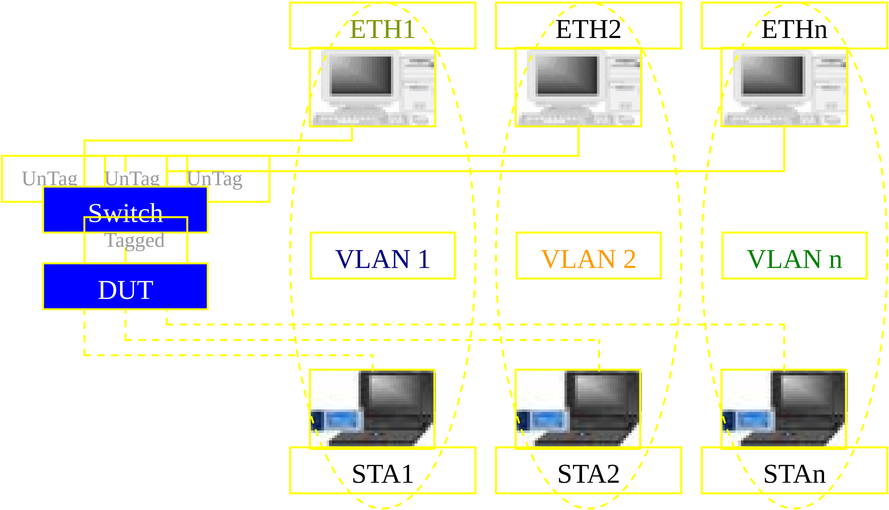
• Uplink Speed Limit (1-1687): It indicates the transmission rate.

VAP / VLAN Settings

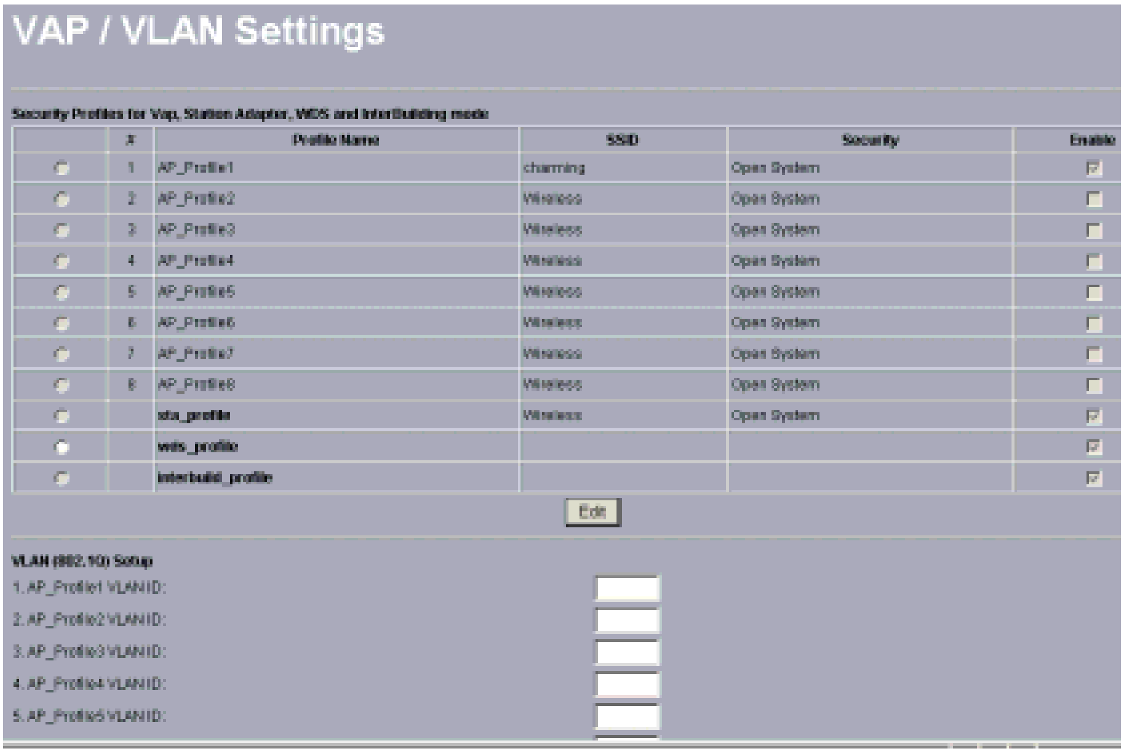
Overview

As the number of data-based systems increase, it becomes more and more difficult to provide the network infrastructure (due to the sheer number of Ethernet connections that need to be provided) from the perspective of cost, space, and wire management. Luckily, the advent technology called VLAN (Virtual Local Area Network) can achieve her mission. Now it is possible for these multi devices to be multi devices in function without the need for multiple physical network APs.

See the diagram below.



Under this mode, the FT213 access point can be have as 8 virtual Wireless LAN infrastructures. You can specify unique SSID for these different infrastructures. For example, VLAN1 contains ETH1 and STA1, VLAN2 contains ETH2 and STA2, and so on. However, they all share the same and undertake different tasks. Some VLANs can be used for guest Internet access, others for enterprise users, and administrators can be put on a high security VLAN with enhanced firewall permissions. All this can be achieved using a single infrastructure to emulate up to 8 infrastructures. The AP does this by assigning each of the 8 VLANs it's own SSID, so you will think you are looking at up to 8different wireless networks.



VAP / VLAN Settings

Security Profiles for Vap, Station Adapter, WDS and InterBuilding mode

	#	Profile Name	SSID	Security	Enable
○	1	AP_Profile1	charming	Open System	☑
○	2	AP_Profile2	Wireless	Open System	☐
○	3	AP_Profile3	Wireless	Open System	☐
○	4	AP_Profile4	Wireless	Open System	☐
○	5	AP_Profile5	Wireless	Open System	☐
○	6	AP_Profile6	Wireless	Open System	☐
○	7	AP_Profile7	Wireless	Open System	☐
○	8	AP_Profile8	Wireless	Open System	☐
○		sta_profile	Wireless	Open System	☑
●		wds_profile			☑
○		interbuild_profile			☑

Edit

VLAN (802.1Q) Setup

1. AP_Profile1 VLANID:

2. AP_Profile2 VLANID:

3. AP_Profile3 VLANID:

4. AP_Profile4 VLANID:

5. AP_Profile5 VLANID:

Figure 5-2

You can configure each profile by clicking "Edit". Such configuration as configuring profile name, SSID, enabling "broadcast SSID", or doing security.

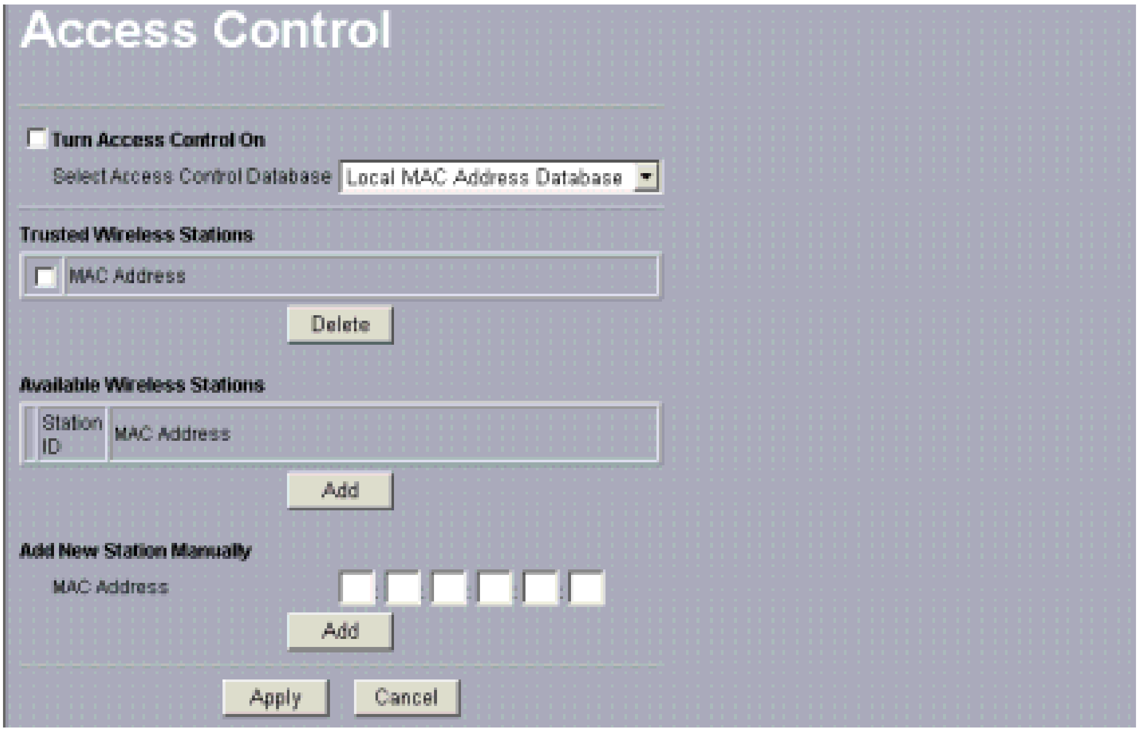
Understanding WEP/WPA Security Options

The following elaborate WEP/WPA security options.

Field	Description
Network Authentication	You have two authentication options. • Open System: No authentication is imposed to the AP. However, if the 802.1x option is configured, authentication of connections can be performed by a RADIUS server. • Shared: this is for shared key authentication. Data is encrypted.
Encryption Strength	You can select the following data encryption options: Disabled 64- 128- or 152-bit WEP With Open System Authentication and 64- 128- or 152-bit WEP Data Encryption with Shared Key authentication
Security Encryption (WEP) Keys	WEP enabled, you can manually enter the four data encryption keys or enable Passphrase to generate the keys automatically. These values must be matched between all Clients and access points at your LAN (key 1 must be the same for all, key 2 must be the same for all, etc.) Two ways to create WEP encryption keys: • Passphrase. Passphrase functions as automatically case-sensitive characters. However not all wireless adapters support passphrase key generation. • Manual. These values are not case sensitive. 64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). 152-bit WEP: enter 32 hexadecimal digits (any combination of 0-9, a-f, or A-F).
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA Pre-Shared-Key uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. It uses Temporal Key Integrity Protocol (TKIP) for encryption keys. However not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.
WPA2-PSK	Identical to WPA-PSK with the exception of the way to encryption keys. WPA2-PSK uses Advanced Encryption Standard(AES) for encryption keys.
WPA-PSK & WPA 2-PSK	You may have the option of WPA-PSK associated with TKIP. Alternatively, you can select WPA2-PSK associated with AES.

Access Control

Authentication by username and password is only part of the story. Frequently you want to let people in based on something other than who they are. Something such as where they are coming from. Restricting access based on something other than the identity of the user is generally referred to as Access Control.



Access Control

□ Turn Access Control On

Select Access Control Database: Local MAC Address Database

Trusted Wireless Stations

□	MAC Address

Available Wireless Stations

	Station ID	MAC Address

Add New Station Manually

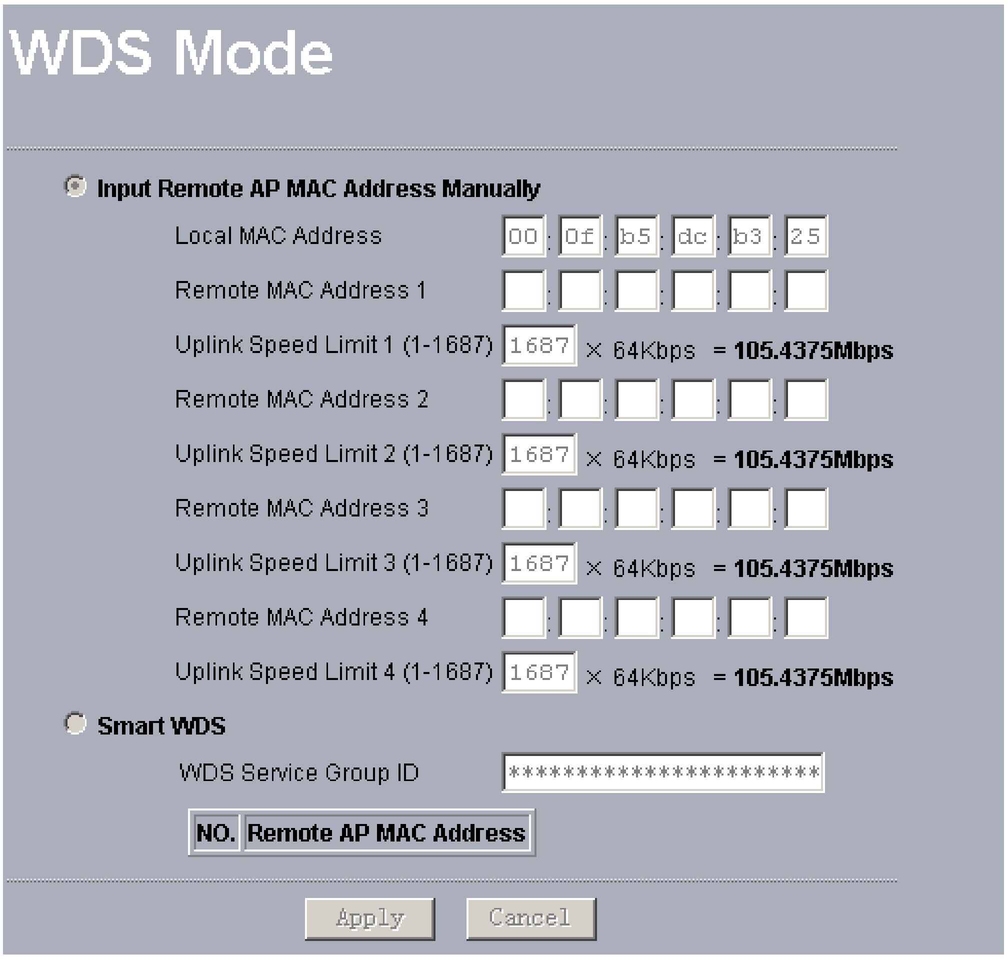
MAC Address □:□:□:□:□:□

Figure: 5-3

You can restrict access to only trusted STAs so that unknown STAs cannot wirelessly connect to the FT213 by turning Access Control on.
By entering MAC Address of new stations, you can manually add the stations to allow them to be connected to the FT213.

WDS Mode

In a Wireless Distribution System (WDS) mode, multiple access points can be configured to operate in the WDS mode to inter-connect wired LAN segments that are attached to the FT213 access point. Up to four devices can be connected to the FT213.



WDS Mode

● Input Remote AP MAC Address Manually

Local MAC Address 00 : 0f : b5 : dc : b3 : 25

Remote MAC Address 1 □ : □ : □ : □ : □ : □

Uplink Speed Limit 1 (1-1687) 1687 × 64Kbps = 105.4375Mbps

Remote MAC Address 2 □ : □ : □ : □ : □ : □

Uplink Speed Limit 2 (1-1687) 1687 × 64Kbps = 105.4375Mbps

Remote MAC Address 3 □ : □ : □ : □ : □ : □

Uplink Speed Limit 3 (1-1687) 1687 × 64Kbps = 105.4375Mbps

Remote MAC Address 4 □ : □ : □ : □ : □ : □

Uplink Speed Limit 4 (1-1687) 1687 × 64Kbps = 105.4375Mbps

○ Smart WDS

WDS Service Group ID ************************

NO.	Remote AP MAC Address

Figure: 5-4

Local MAC Address:

This field provides the FT213 MAC address.

Remote MAC Address:

Enter the MAC Address of your desired devices connected to the FT213 in WDS Mode.

Uplink Speed Limit:

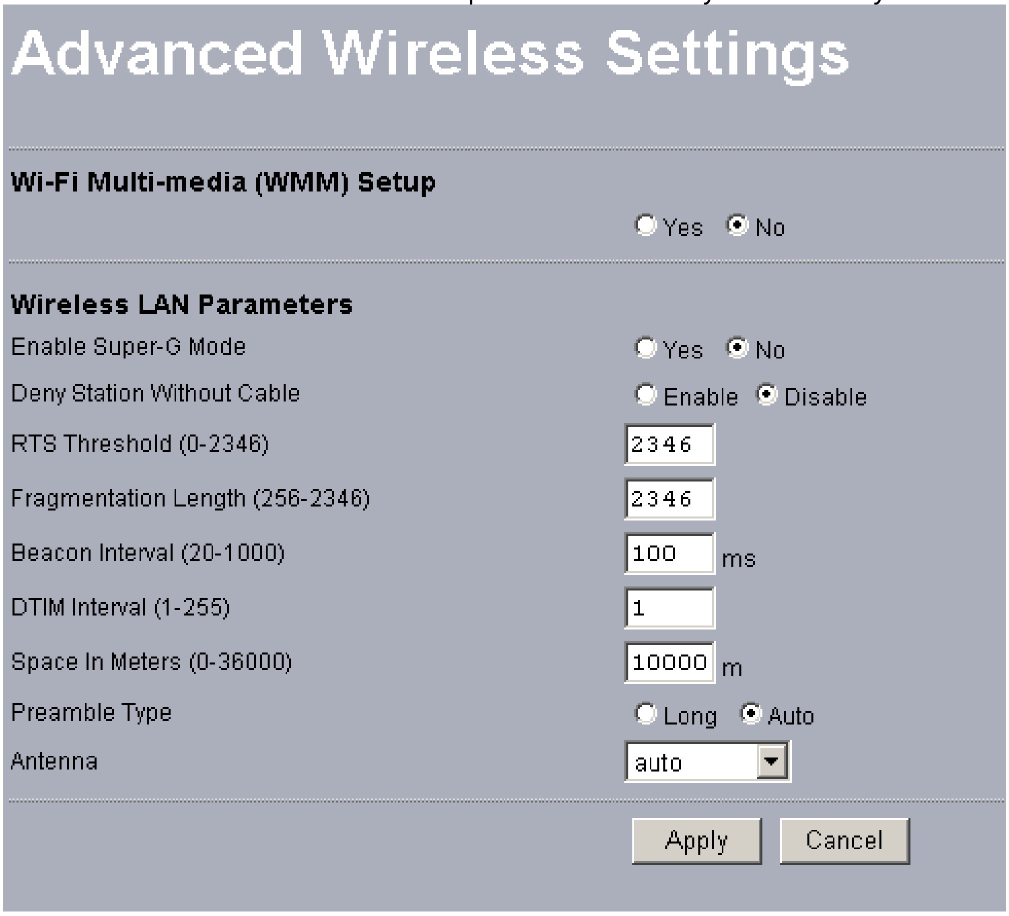
You can specify the transmission rate between the FT213 and other devices by entering the value in uplink speed limit. The most speed available is 1687 ×64Kbps=105.4375Mbps

Smart WDS

Under bridge mode, enabling smart WDS, the FT213 access point can sniff other FT213 around him and automatically connect those that work in the same channel.
WDS Service Group ID
If two APs share the same group ID, they will be automatically connected.
Smart WDS can be activated on the premise that APs must be FT213.

Advanced Settings

The default advanced wireless LAN parameters usually streamline your work.



Advanced Wireless Settings

Wi-Fi Multi-media (WMM) Setup

○ Yes ● No

Wireless LAN Parameters

Enable Super-G Mode	○ Yes ● No
Deny Station Without Cable	○ Enable ● Disable
RTS Threshold (0-2346)	2346
Fragmentation Length (256-2346)	2346
Beacon Interval (20-1000)	100 ms
DTIM Interval (1-255)	1
Space In Meters (0-36000)	10000 m
Preamble Type	○ Long ● Auto
Antenna	auto

Figure: 5-5

Wi-Fi Multi-media (WMM)

Currently interest and demand for multimedia applications and advanced capabilities are growing quickly. In the residential market, Voice over Internet Protocol (VoIP), video streaming, music streaming, and interactive gaming are among the most anticipated applications. In enterprise and public networks, support for VoIP, real time streaming of audio and video content, as well as traffic management, allows network owners to invent advanced methods to offer a richer and more diverse set of services. WMM prioritizes traffic demands from different applications and extends Wi-Fi's high quality end-user experience from data connectivity to voice, music, and video applications under a wide variety of environment and traffic conditions. WMM defines four access categories (voice, video, best effort, and background) that are used to prioritize traffic so that these applications have access to the necessary network resources.

When your STA connect to the FT213, you can enjoy high-quality multimedia function at your LAN, by enabling WMM.

Note

Before enabling WMM, make sure your stations must also support WMM. Further, your operating system must be Windows XP with Service Pack 2.

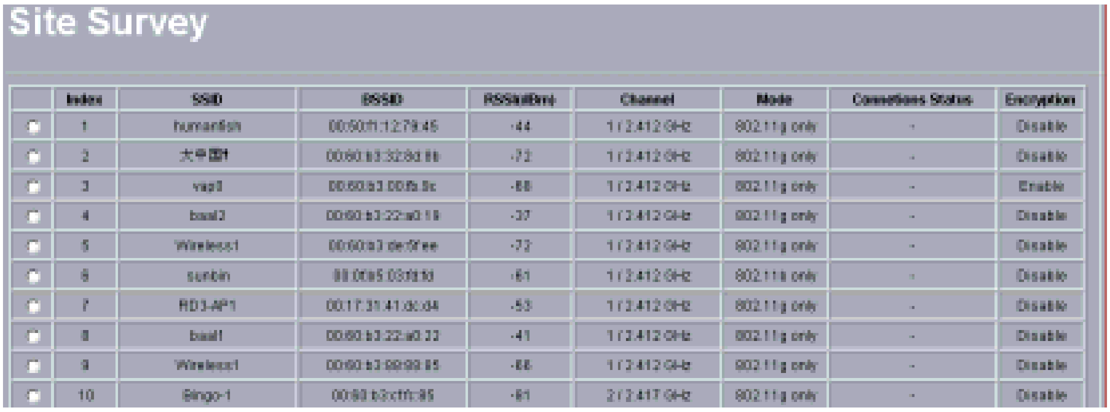
Super-G and Turbo-A wireless parameters

Enabling super-G or Turbo-A, your transmission rate could reach up to 108Mbps.
The following describes the advanced wireless parameters.

Field	**Description**
RTS Threshold	The packet size used to determine whether it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for packet transmission.
Fragmentation Length	This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.
Beacon Interval	Specifies the data beacon rate between 20 and 1000.
DTIM Interval	The Delivery Traffic Indication Message specifies the data beacon rate between 1 and 255.
Preamble Type	A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Long is the default
Antenna	Select the desired antenna for transmitting and receiving. Auto is the default.

Chapter 6: Site Survey and Link Test

Site Survey



Site Survey

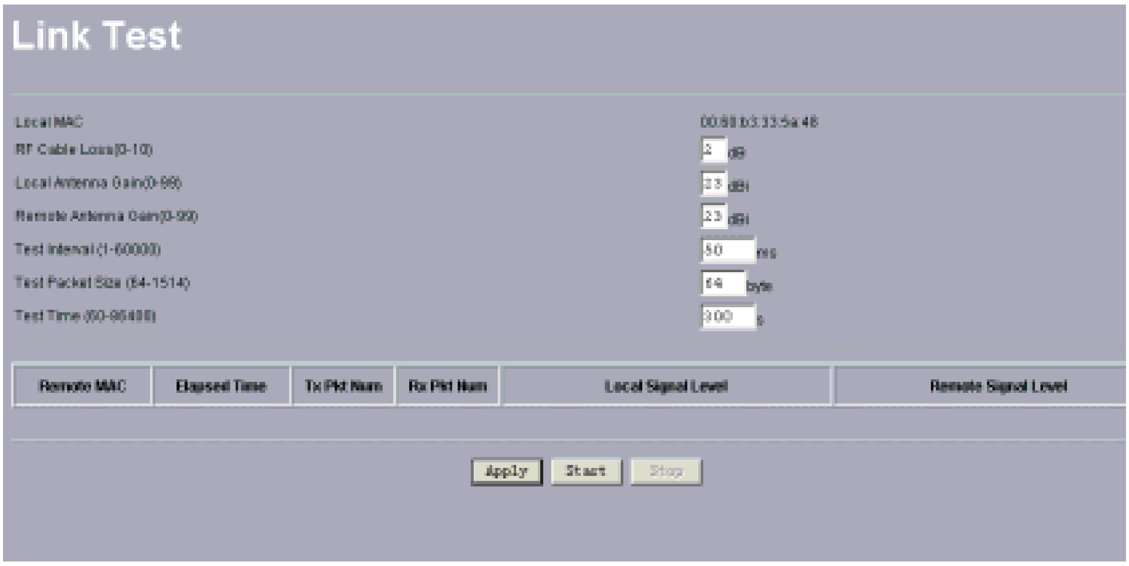
	Index	SSID	BSSID	RSSI(dBm)	Channel	Mode	Connections Status	Encryption
○	1	humanfish	00:50:f1:12:79:45	-44	1 / 2.412 GHz	802.11g only	-	Disable
○	2	大中国	00:60:b3:32:8d:86	-72	1 / 2.412 GHz	802.11g only	-	Disable
○	3	vap3	00:60:b3:00:fb:5c	-68	1 / 2.412 GHz	802.11g only	-	Enable
○	4	basil2	00:60:b3:22:a0:18	-37	1 / 2.412 GHz	802.11g only	-	Disable
○	5	Wireless1	00:60:b3:de:5f:ee	-72	1 / 2.412 GHz	802.11g only	-	Disable
○	6	sunbin	00:0f:a5:03:fd:fd	-61	1 / 2.412 GHz	802.11b only	-	Disable
○	7	RD3-AP1	00:17:31:41:dc:d4	-53	1 / 2.412 GHz	802.11g only	-	Disable
○	8	basil1	00:60:b3:22:a0:22	-41	1 / 2.412 GHz	802.11g only	-	Disable
○	9	Wireless1	00:60:b3:99:99:85	-66	1 / 2.412 GHz	802.11g only	-	Disable
○	10	Bingo-1	00:60:b3:cf:fc:85	-61	2 / 2.417 GHz	802.11g only	-	Disable

Figure: 6-1

Site Survey provides you with a table of adjacent APs connected to your FT213 , when it acts as a station. In terms of each connected AP, Site Survey offers you their personal information, including SSID, BSSID, RSSI, channel mode, connection status and encryption.

Link Test

To optimize the communication between your LAN, link test is designed to test the parameters that indicates communication quality.



Link Test

Local MAC	00:60:b3:33:5a:48
RF Cable Loss(0-10)	2 dB
Local Antenna Gain(0-99)	23 dBi
Remote Antenna Gain(0-99)	23 dBi
Test Interval (1-60000)	50 ms
Test Packet Size (64-1514)	64 byte
Test Time (60-86400)	300 s

Remote MAC	Elapsed Time	Tx Pkt Num	Rx Pkt Num	Local Signal Level	Remote Signal Level

Figure: 6-2

We'll discuss parameters in link test.

RF Cable Loss(0-10):

This indicates RF loss in cables, ranging from 0 to 10.

Local Antenna Gain(0-99):

This indicates extended coverage provided by the local , for an existing 802.11a/b/g wireless local area network (WLAN), ranging from o to 99.

Remote Antenna Gain((0-99):

This indicates extended coverage provided by the remote , for an existing 802.11a/b/g wireless local area network (WLAN).ranging from o to 99.

Test Interval (1-60000): This provides testing time

Test Packet Size (64-1514):

This tests the size of packet transmitted between the two access points, ranging from 64 to 1514

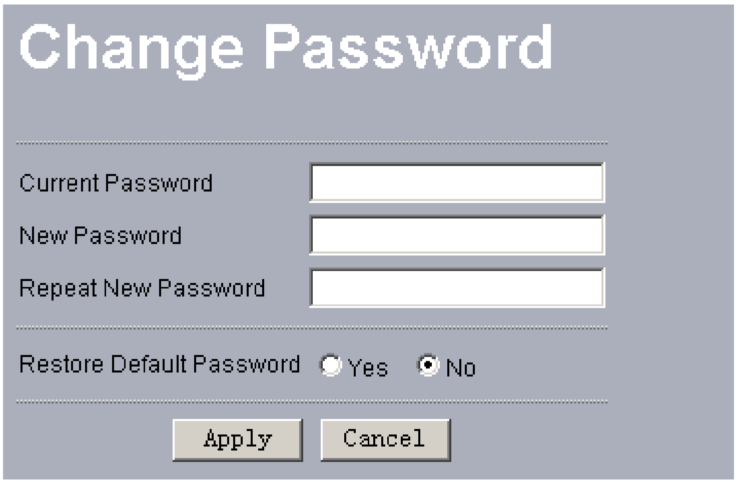
Test Time (60-86400):

This specifies how long the linking test will last ranging from 60 to 86400.

Chapter 7: Management

This chapter describes how to manage your FT213 access point.

Change Password



Change Password

Current Password

New Password

Repeat New Password

Restore Default Password ○ Yes ● No

Figure: 7-1

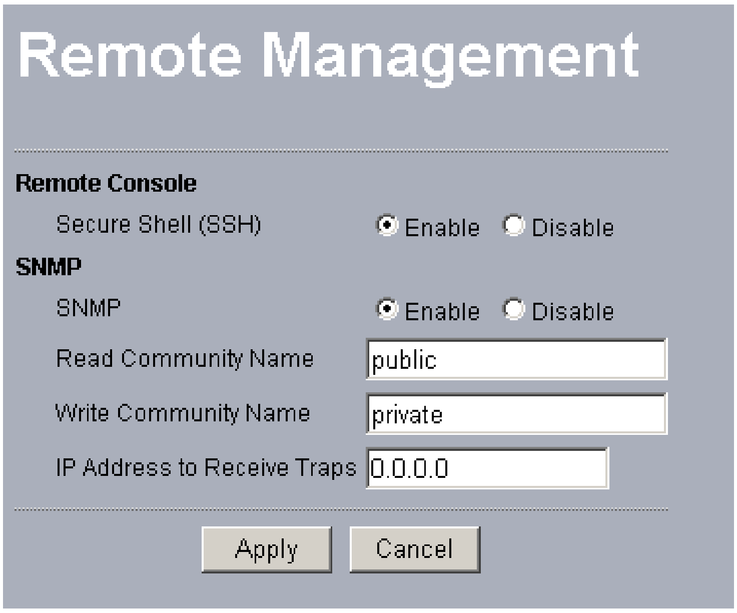
You can have your desired password by changing password.
Take the following steps to change password.

•Enter your currently-used password in the current field.
•Enter your new password in the New Password field.
•Re-enter the new password to confirm it in the Repeat New Password field.

Finally, click “Apply” to save the change.
Also, if you desire to restore to the factory-set password, please click “Yes”.
The default setting is disabled.

Remote Management

FT213 provides remote management to manage and diagnose your network.



Remote Management

Remote Console

Secure Shell (SSH) ● Enable ○ Disable

SNMP

SNMP ● Enable ○ Disable

Read Community Name: public

Write Community Name: private

IP Address to Receive Traps: 0.0.0.0

Figure: 7-2

SSH

Secure Shell (SSH) is a program that provides a cryptographically secure replacement for Telnet that is considered the de facto protocol for remote logins. SSH runs in the Application Layer of the TCP/IP stack. SSH provides a secure connection over the Internet providing strong user authentication. SSH protects the privacy of transmitted data (such as passwords, binary data, and administrative commands) by encrypting it. SSH clients make SSH relatively easy to use and are available on most computers including those that run Windows or a type of UNIX. SSH clients are also available on some handheld devices.

SSH on FT213 is enabled by default. When user manager is enabled, SSH uses the same usernames and passwords established by the user manager.

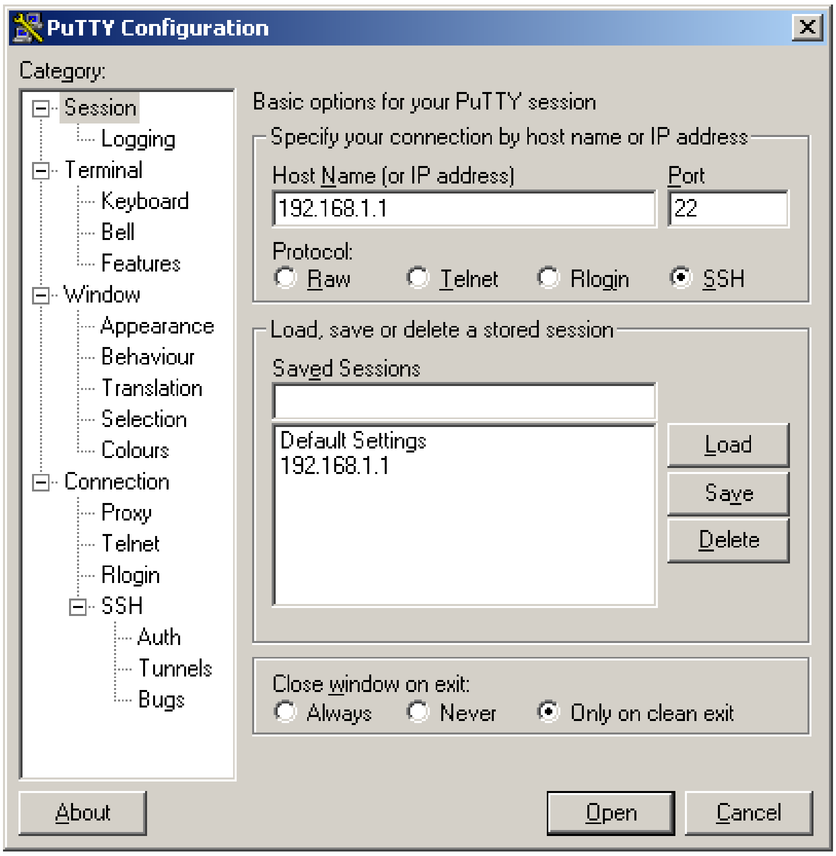
The applicability of SSH for the FT213 access point allows you to have insight into your LAN.

Note

If your computer does not have the SSH client installed, you must procure and install it before you can proceed. You can download the latest SSH client from the following site: http://ssh.com/.

Take the following steps to manage the FT213 via SSH..

From the Putty Configuration, enter IP address in host name field and port number in port field. Also, select SSH as protocol.



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.1

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

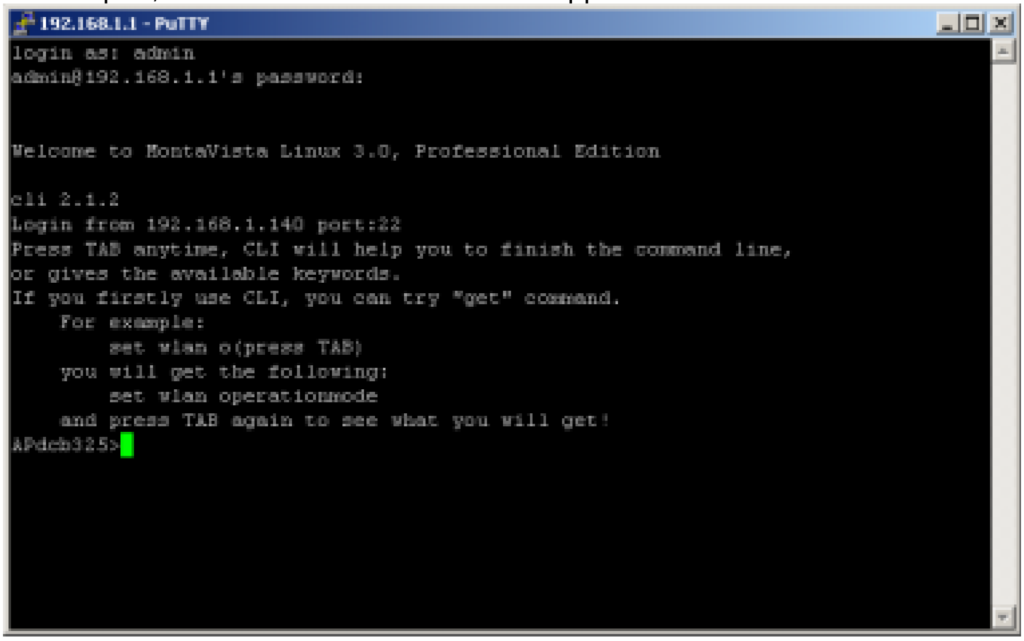
Saved Sessions

Default Settings
192.168.1.1

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure: 7-3

Press Open, and the screen below should appear.



```
login as: admin
admin@192.168.1.1's password:


Welcome to MontaVista Linux 3.0, Professional Edition

cli 2.1.2
Login from 192.168.1.140 port:22
Press TAB anytime, CLI will help you to finish the command line,
or gives the available keywords.
If you firstly use CLI, you can try "get" command.
    For example:
        set wlan o(press TAB)
    you will get the following:
        set wlan operationmode
    and press TAB again to see what you will get!
APdcb325>
```

Figure: 7-4

The login name is admin and password is the default password. After successful login, the screen should show the APdcb325>. In this example, the APdcb325 is the FT213 access point name.. Enter help to display the SSH command help.

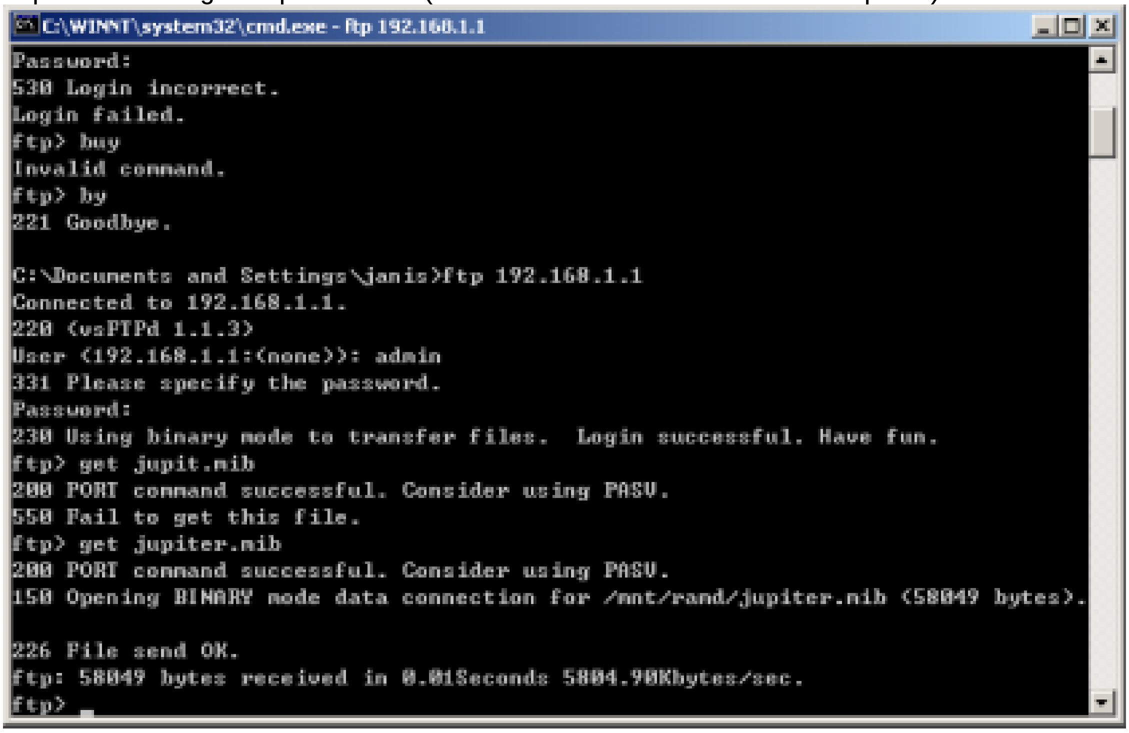
SNMP

SNMP (simple network management protocol) is a distributed-management protocol. Via SNMP, you have access to administrate your remotely. Read Community Name: You have access to read rather than write.The default name is public.

Write Community Name: The default name is private.

Take the steps below to manage your FT213 via SNMP.

Enter ftp 192.168.1.1 , then in turn enter admin and password, and finally enter get Jupiter. mib to get Jupiter. MIB. (The FT213’s software is called Jupiter.)



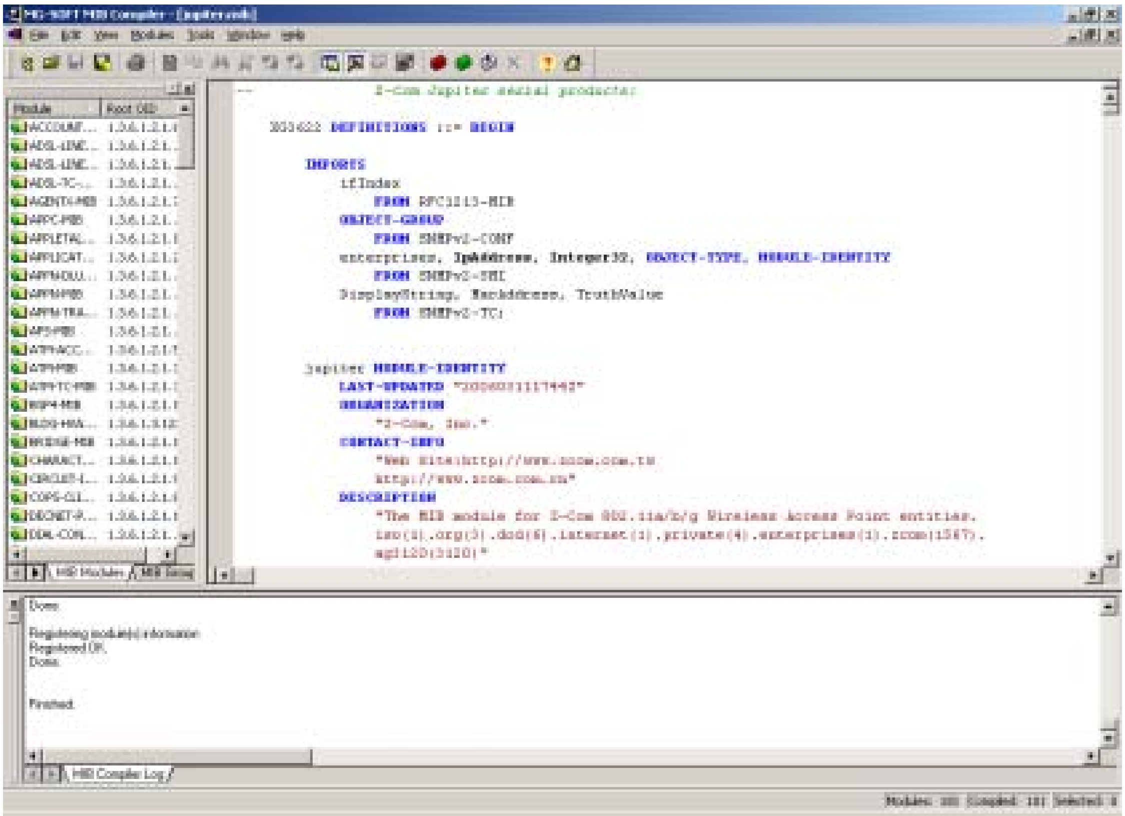
```
Password:
530 Login incorrect.
Login failed.
ftp> buy
Invalid command.
ftp> by
221 Goodbye.

C:\Documents and Settings\janis>ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 1.1.3)
User (192.168.1.1:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files.  Login successful. Have fun.
ftp> get jupit.mib
200 PORT command successful. Consider using PASV.
550 Fail to get this file.
ftp> get jupiter.mib
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for /mnt/rand/jupiter.mib (58049 bytes).

226 File send OK.
ftp: 58049 bytes received in 0.01Seconds 5804.90Kbytes/sec.
ftp> _
```

Figure: 7-5

From MIB Compiler interface, open jupter.mib and compile the file by enabling compile Jupiter mib on tools menu. Save the compiled files to your disk.



MG-SOFT MIB Compiler - [jupiter.mib]
File Edit View Modules Tools Window Help
MIB Modules
MIB Tree
MIB Compiler Log

Module	Root OID
ACCOUNT...	1.3.6.1.2.1....
ADSL-LINE...	1.3.6.1.2.1....
ADSL-LINE...	1.3.6.1.2.1....
ADSL-TC-...	1.3.6.1.2.1....
AGENTX-MIB	1.3.6.1.2.1....
APPC-MIB	1.3.6.1.2.1....
APPLETAL...	1.3.6.1.2.1....
APPLICAT...	1.3.6.1.2.1....
APPN-DLU...	1.3.6.1.2.1....
APPN-MIB	1.3.6.1.2.1....
APPN-TRA...	1.3.6.1.2.1....
APS-MIB	1.3.6.1.2.1....
ATM-ACC...	1.3.6.1.2.1....
ATM-MIB	1.3.6.1.2.1....
ATM-TC-MIB	1.3.6.1.2.1....
BGP4-MIB	1.3.6.1.2.1....
BLDG-HVA...	1.3.6.1.3.12...
BRIDGE-MIB	1.3.6.1.2.1....
CHARACT...	1.3.6.1.2.1....
CIRCUIT-I...	1.3.6.1.2.1....
COPS-CLI...	1.3.6.1.2.1....
DECNET-P...	1.3.6.1.2.1....
DIAL-CON...	1.3.6.1.2.1....

```
--          Z-Com Jupiter serial products:

    3003622 DEFINITIONS ::= BEGIN

        IMPORTS
            ifIndex
                FROM RFC1213-MIB
            OBJECT-GROUP
                FROM SNMPv2-CONF
            enterprises, IpAddress, Integer32, OBJECT-TYPE, MODULE-IDENTITY
                FROM SNMPv2-SMI
            DisplayString, MacAddress, TruthValue
                FROM SNMPv2-TC;


        jupiter MODULE-IDENTITY
            LAST-UPDATED "200603111744Z"
            ORGANIZATION
                "Z-Com, Inc."
            CONTACT-INFO
                "Web Site:http://www.zcom.com.tw
                http://www.zcom.com.tw"
            DESCRIPTION
                "The MIB module for Z-Com 802.11a/b/g Wireless Access Point entities.
                iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).zcom(1567).
                ag1120(3120)"
```

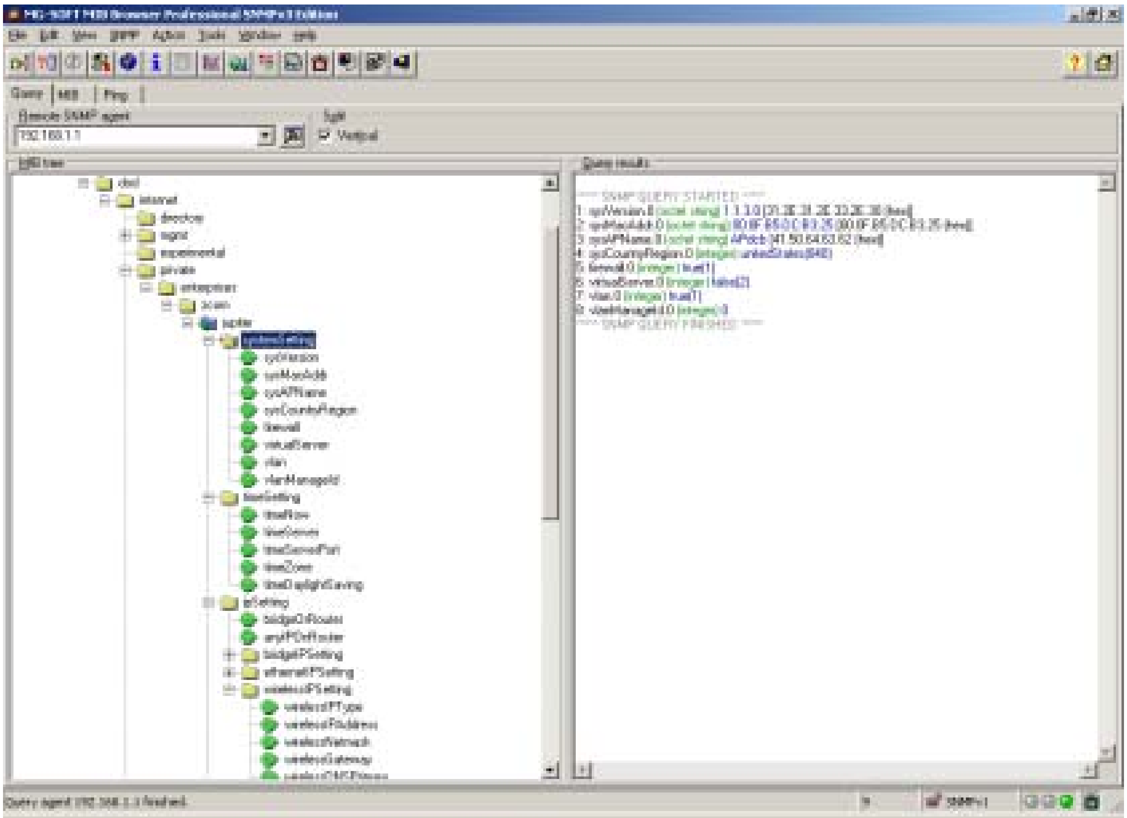
```
Done.

Registering module(s) information
Registered OK.
Done.

Finished.
```

Figure: 7-6

Load the file to SNMP station. Your screen will appear.



```
***** SNMP QUERY STARTED *****
1: sysVersion.0 (octet string) 1.1.3.0 [31.2E.31.2E.33.2E.30 (hex)]
2: sysMacAddr.0 (octet string) 00:0F:B5:0C:83:25 [00.0F.B5.0C.83.25 (hex)]
3: sysAPName.0 (octet string) APdcb [41.50.64.63.62 (hex)]
4: sysCountryRegion.0 (integer) unitedStates(840)
5: firewall.0 (integer) true(1)
6: virtualServer.0 (integer) false(2)
7: vlan.0 (integer) true(1)
8: vlanManageId.0 (integer) 0
***** SNMP QUERY FINISHED *****
```

Query agent 192.168.1.1 finished.

Figure: 7-7

4 Changing settings with the database query page

Follow these steps to change an access point setting from the Database Query page:

Step 1 Click Get. The current value for the setting appears in the Value field.

Step 2 Modify the value in the Value field.

Step 3 Click Set. The new value is set on FT213.

Upgrade Firmware

Note

When uploading software to the FT213 Access Point, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, and render the FT213 completely inoperable.

The software of the FT213 is stored in FLASH memory, and can be upgraded as new software is released by . Upgrade files can be downloaded from Comtec's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.RMG) file before sending it to the wireless access point. The upgrade file can be sent using your browser.

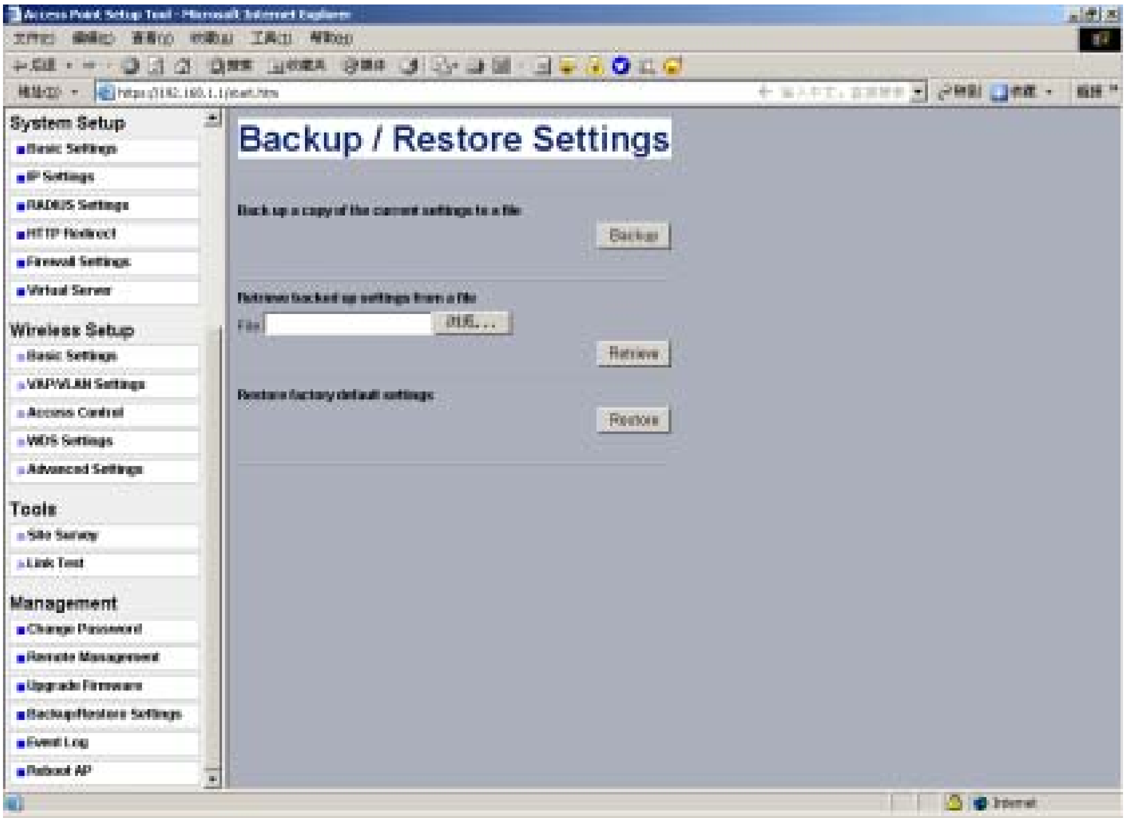
Note

The Web browser used to upload new firmware into the FT213 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

1. Download the new software file from www.comtec.com.tw , save it to your hard disk, and unzip it.
2. From the main menu Management section, click the Upgrade Firmware link to display the screen above.
3. In the Upgrade Firmware menu, click the Browse button and browse to the location of the image (.RMG) upgrade file.
4. Click Upload. When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about one minute. In some cases, you may need to reconfigure the wireless access point after upgrading.

Backup / Restore Settings

FT213 access point provides backup and restore for file management.



Back up a copy of the current settings to a file

Retrieve backed up settings from a file

Restore factory default settings:

Figure: 7-8

You have access to back up the currently settings by enabling FT213's Backup function.

Retrieve:

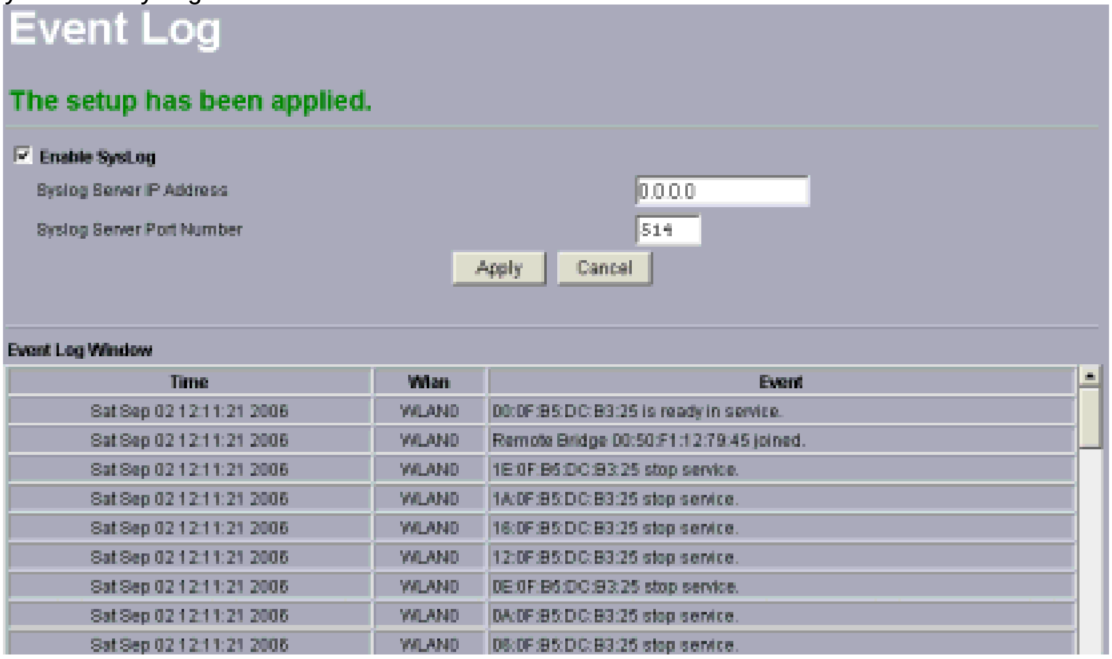
Retrieve button allows you to retrieve your backup files.

Restore:

This button can be used to clear ALL data and restore ALL settings to the factory default values.

Event Log

If you have a SysLog server on your LAN, enable the SysLog option. Event Log offers you activity log information.



Event Log

The setup has been applied.

☑ Enable SysLog

Syslog Server IP Address: 0.0.0.0

Syslog Server Port Number: 514

Event Log Window

Time	Wlan	Event
Sat Sep 02 12:11:21 2006	WLAN0	00:0F:B5:DC:B3:25 is ready in service.
Sat Sep 02 12:11:21 2006	WLAN0	Remote Bridge 00:50:F1:12:79:45 joined.
Sat Sep 02 12:11:21 2006	WLAN0	1E:0F:B6:DC:B3:25 stop service.
Sat Sep 02 12:11:21 2006	WLAN0	1A:0F:B5:DC:B3:25 stop service.
Sat Sep 02 12:11:21 2006	WLAN0	16:0F:B5:DC:B3:25 stop service.
Sat Sep 02 12:11:21 2006	WLAN0	12:0F:B5:DC:B3:25 stop service.
Sat Sep 02 12:11:21 2006	WLAN0	0E:0F:B6:DC:B3:25 stop service.
Sat Sep 02 12:11:21 2006	WLAN0	0A:0F:B5:DC:B3:25 stop service.
Sat Sep 02 12:11:21 2006	WLAN0	06:0F:B5:DC:B3:25 stop service.

Figure: 7-9

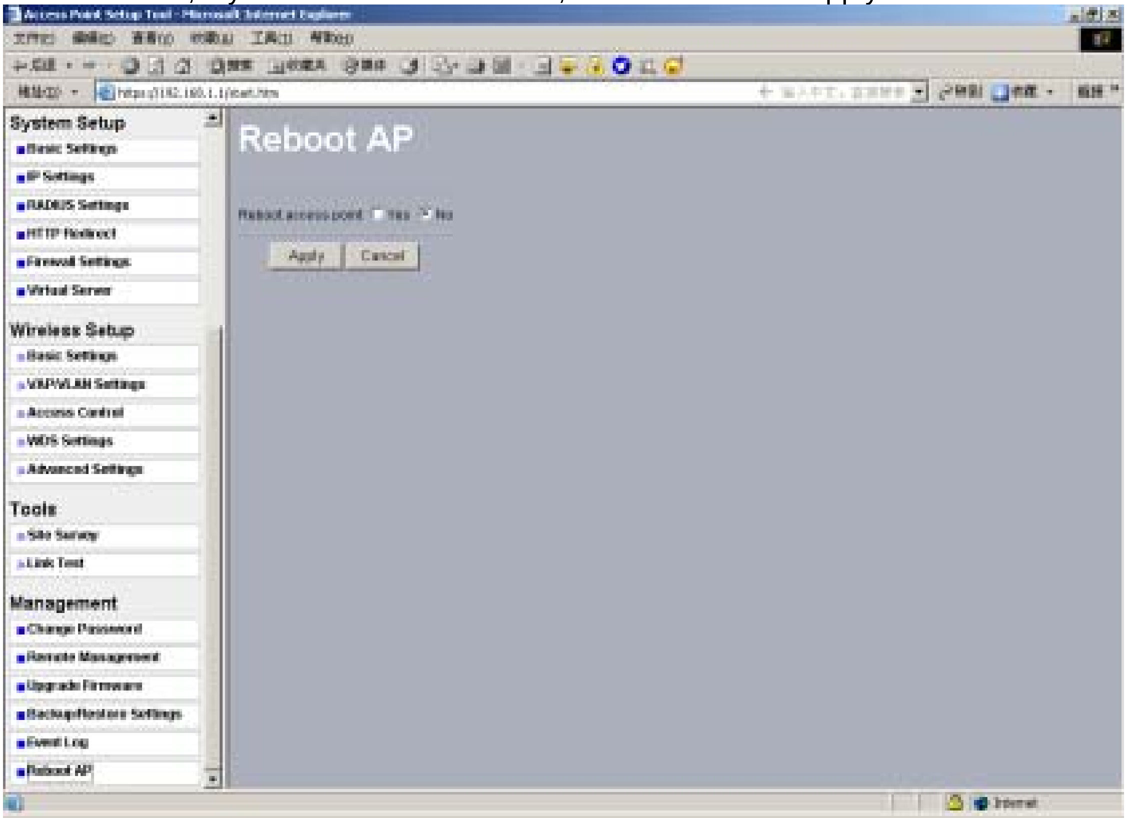
- SysLog Server IP address:

FT213 will send all the SysLog to the specified IP address if SysLog option is enabled. Default: 0.0.0.0

- Port: The port number configured in the SysLog server on your network. Default: 514

Reboot AP

In some cases, if you want to reboot FT213, click Yes and then apply. FT213 will reboot.



Reboot AP

Reboot access point ○ Yes ● No

Figure: 7-10

Chapter 8: Warranty Information

LIMITED WARRANTY

Comtec warrants to You that, for a period of one year (the “Warranty Period”), your ’s Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and ' entire liability under this warranty will be for at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to pays for UPS Ground shipping from back to You only.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED

TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS ANDWARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED.

Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives you specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by , (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by , or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL BE LIABLE FOR ANY LOST DATA, REVENUE OR

PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY

OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT

(INCLUDING ANY SOFTWARE), EVEN IF FT213 HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT

WILL ’ LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: sales@comtec.com.tw

Chapter 9: Regulatory Information

FCC Statement

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

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjuction with any other antenna or transmitter.

To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

Safety Notices

Do not use this product near water, for example, in a wet basement or near a swimming pool. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Chapter 10: Technical Support

Manufacturer's Statement

The FT213 is provided with warranty. It is not desired or expected that the user open the device. If malfunction is experienced and all external causes are eliminated, the user should return the unit to the manufacturer and replace it with a functioning unit.
If you are experiencing trouble with this unit, the point of contact is:
support@comtec.com.tw
+886-2-8221 8815 (Monday - Friday, 9am to 6pm EST)
or visit our website at
www.comtec.com.tw