



ALL-WAPC0450C

Wireless Controller for WAP-C-AccessPoints



USER MANUAL

Table of Contents

Product Overview.....	7
Captive Portal.....	73
Getti Guest Account.....	75
Installing the Switch.....	15
Management Interface.....	15
Connecting the Switch to a Network.....	16
Software Features.....	18
Using the Switch.....	19
Wireless Controller Features	20
Managing C-Series-AccessPoints	20
Device Management.....	22
Summary.....	22
Access Points.....	24
Access Point Settings.....	29
AP Groups.....	42
Access Control	44
Wireless Services.....	46
Monitor	47
Active Clients.....	47
Rogue AP Detection.....	49
System Log.....	51
Email Alert.....	56
Visualization	60
Topology View.....	60
Map View	63
Floor View	65
Statistics	70
Access Points.....	70
Wireless Clients.....	71
Real Time Throughput.....	72
Hotspot Services	73
Maintenance	76

Schedule Tasks.....	76
Troubleshooting.....	77
Bulk Upgrade.....	78
SSL Certificate	82
Check Codes	84
Ethernet Switch Features	86
System.....	86
Summary	86
IP Settings.....	87
System Time.....	90
Port Settings.....	92
EEE	97
Management	140
System Information	140
User Management.....	141
Dual Image	142
Diagnostics.....	195
Cable Diagnostics	195
Ping Test.....	196
IPv6 Ping Test.....	197
Trace Route.....	198

Installing the Switch

This section will guide you through the installation process.

Management Interface

The Switch features an embedded Web interface for the monitoring and management of your device.

Management Interface Default Values

IP Address: 192.168.1.239

Username: admin

Password: admin

Connecting the Switch to a Network

Discovery in a Network with a DHCP server

Use the procedure below to setup the Switch within a network that uses DHCP.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000Mbps) Ethernet port on the Switch front panel and the other end to the Ethernet port on the computer. Verify that the LED on the Ethernet ports of the Switch are **Green**.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connection**. Select **Internet Protocol Version 4 (TCP/IPv4)**. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.0.10 and the Subnet mask address as 255.255.255.0).
5. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and press **Enter**.
6. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**. To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.
7. Click **IP Settings** under the **System tab** and select IPv4 or IPv6.
8. Click **DHCP** under Auto-Configuration.
9. Click **Apply** to save the settings.
10. Connect the Switch to your network (DHCP enabled).
11. On the DHCP server, find and write down the IP address allocated to the device. Use this IP address to access the management interface.

Discovery in a Network with a DHCP server

This section describes how to set up the Switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your Switch in order to log in to the web-based management interface.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the Power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute or so for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000Mbps) Ethernet port on the Switch front panel and the other end to Ethernet port on the computer. Verify that the LED on Ethernet ports of the Switch are **Green**.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connection**. Select **Internet Protocol Version 4 (TCP/IPv4)**.
5. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: **192.168.0.239** and the Subnet mask address as **255.255.255.0**).
6. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and press **Enter**.
7. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**. To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.
8. Click **IP Settings** under the **System menu** and select **Static IP** to configure the IP settings of the management interface.
9. Enter the IP address, Subnet mask, and Gateway.
10. Click **Apply** to update the system.

Software Features

Using the Switch

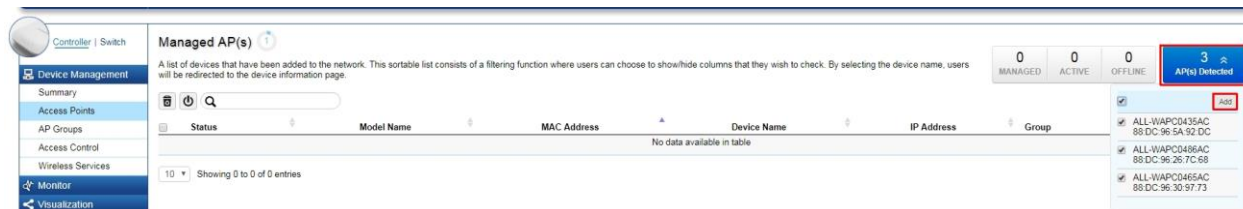
Besides the functions of a Wireless Controller, the Controller also possesses functions of a full-featured Layer 2 Ethernet Switch. Use the Controller / Switch tab on the upper left corner of the user interface to toggle between the Wireless Controller or Layer 2 Switch functions.



Wireless Controller Features

Managing C-Series Access Points

1. Access Points in the network will be automatically discovered by the Controller and will be listed under the AP(s) Detected list in the Access Point menu.



2. Select the Access Point(s) you wish to manage and click **Add**.



3. You will be prompted to assign the IP Address under the IP Assignment screen.

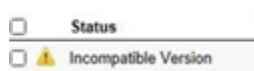


Auto-Configuration	<p>DHCP: You can choose to auto assign IP address if there is a DHCP server in the network.</p> <p>Static: If you wish to manually assign the IP address, choose Static. Enter the IP address you wish to assign to the AP and fill in the subnet mask, default gateway and DNS server address.</p> <p>Keep AP's Settings: Select this option for the AP to use its current network settings.</p>
IP Address	Enter the IP address for the Access Point.
Subnet Mask	Enter the subnet mask for the Access Point.
Default Gateway	Enter the default gateway for the Access Point.
Primary DNS Server	Enter the primary DNS server name.
Secondary DNS Server	Enter the secondary DNS server name (if necessary).

- Click Apply and the Access Point(s) you've configured will be moved to the Managed list. Note that the status of the AP will change from **Connecting** to **Provisioning** to **Online**. Once the status turns **Online**, your Access Point(s) have been successfully added to the Managed list.

Status	Model Name	MAC Address	Device Name	IP Address	Group
<input type="checkbox"/> Online	ALL-WAPC0486AC	88 DC 96 26 7C 68	ALL-WAPC0486AC	192.168.2.116	
<input type="checkbox"/> Online	ALL-WAPC0465AC	88 DC 96 30 97 73	ALL-WAPC0465AC	192.168.2.115	
<input type="checkbox"/> Online	ALL-WAPC0435AC	88 DC 96 5A 92 DC	ALL-WAPC0435AC	192.168.2.114	

Note: If the status shows **Incompatible Version**, please check and make sure that the firmware of the Access Point and Switch are compatible.



Device Management

Summary

The Summary page shows general system information for the Controller including the Controller Status, the software version, the maximum number of APs the system can manage, MAC Address, IP Address, serial number, and system uptime for the system.

Dashboard

The Dashboard on the upper right corner of the GUI shows the current status of C-Series-AP that has been managed by the ALL-WAPC0450C Controller.

6	6	0	13
MANAGED	ACTIVE	OFFLINE	CLIENTS

Managed	This shows the number of APs currently managed by the ALL-WAPC0450C.
Active	This shows the number of managed APs that currently have an active connection with the ALL-WAPC0450C.
Offline	This shows the number of managed APs that currently do not have an active connection with the ALL-WAPC0450C.
Clients	This shows the total number of wireless clients currently connected to all the managed APs.

Controller State

Status: Select whether to Enable or Disable the Controller feature on the Switch.

Click *Apply* to save the changes to the system.

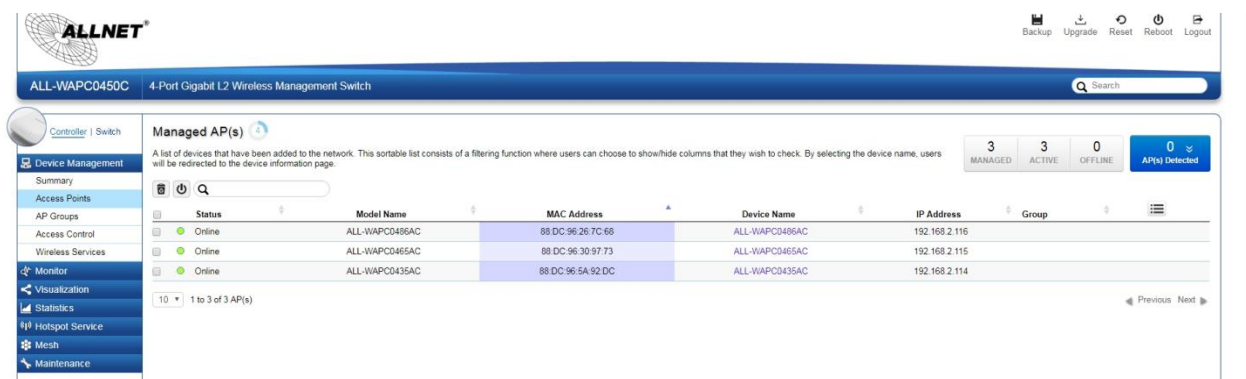
System Information

- Controller Version: This is the software version of the device.
- Max. Managed APs: The maximum number of APs the device is able to manage.
- IP Address: Displays the IP address of the device.
- Base MAC Address: Universally assigned network address.
- Serial Number: Displays the serial number of the device.
- System Uptime: Displays the number of days, hours, and minutes since the last system restart.

Access Points

This page displays the status of all C-Series-AccessPoints that your Controller is currently managing as well as all the C-Series-AccessPoints in the network that the Controller has discovered. Use this page to add C-Series-AccessPoints to your EWS Controller Access Point list.

The ALL-WAPC0450C is able to manage supported C-Series-Access Points. For the discovery procedure to succeed, the ALL-WAPC0450C and the C-Series-Access Point must be connected in the same network. The ALL-WAPC0450C can discover supported C-Series-AccessPoints with any IP address and Subnet settings.



Status	Model Name	MAC Address	Device Name	IP Address	Group
Online	ALL-WAPC046AC	88 DC 96 26 7C 68	ALL-WAPC046AC	192.168.2.116	
Online	ALL-WAPC0465AC	88 DC 96 30 97 73	ALL-WAPC0465AC	192.168.2.115	
Online	ALL-WAPC0435AC	88 DC 96 5A 92 DC	ALL-WAPC0435AC	192.168.2.114	

Managing Access Points

C-Series-AccessPoints can either be configured individually or configured as a group.

To manage an Access Point individually, click on the **Device Name** field of the Access Point you wish to configure and you will be directed to a screen where you can configure settings for the Access Point.

To manage Access Points as a group, go to **Device Management > AP Clusters** to create an AP group and add members into the group. Click on the **Group** field of the AP you wish to configure and you will be directed to a screen where you can configure settings for the AP Group.

Group settings can be overridden by individual AP settings. For example, if you want to set the transmit power to a lower setting for only a few specific APs, leave the Transmit Power at Auto in the Wireless

Radio Settings of the AP Group, then click on the **Device Name** field of the Access Point (which is already in a group) you wish to configure and you will be directed to a screen where you can configure override settings for the selected Access Point.

Refresh Countdown Timer

This is the time left before the page auto-refreshes. The countdown is from 15 seconds.



Dashboard

The Dashboard shows the current status of all the EWS APs that has been managed by the ALL-WAPC0450C.

6	6	0
MANAGED	ACTIVE	OFFLINE

Managed	This shows the number of APs in the managed AP database that are configured with the ALL-WAPC0450C.
Active	This shows the number of managed APs that currently have an active connection with the ALL-WAPC0450C.
Offline	This shows the number of managed APs that currently do not have an active connection with the ALL-WAPC0450C.

AP(s) Detected List

Reveals a list of all APs in the network that the ALL-WAPC0450C automatically discovers. Mouse over the discovered Access Point to show general information such as the MAC address, IP address, model name and firmware version.



Remove AP

The Remove button removes selected Access Point(s) from list. Access Points removed will be automatically set to standalone mode with all settings restored to



their factory default settings.

Reboot AP

The Reboot button will reboot the selected Access Point(s).



Search Bar

Use the Search Bar to search for Access Points managed by the ALL-WAPC0450C using the following criteria: Status, model name, MAC Address, Device name, IP address, Firmware Version, Cluster.



Status

This indicates the current status of the managed Access Point.

Status	Explanation
Online	AP is connected and managed by ALL-WAPC0450C.
Provisioning	AP is currently in the process of connecting to the ALL-WAPC0450C.
Applying Change	AP is currently applying system changes.
Connecting	AP is currently connecting to ALL-WAPC0450C.
Offline	AP is currently offline.

Resetting	AP is resetting.
Firmware Upgrading	AP is currently undergoing firmware upgrade process.
Invalid IP	The subnet of managed AP's IP address is not the same as the ALL-WAPC0450C. Please remove AP and reconfigure AP to the correct setting.
Incompatible Version	AP firmware is not compatible with ALL-WAPC0450C.
Checking Certificate	ALL-WAPC0450C is checking the SSL Certificate of AP.

Model Name

Shows the model name of the managed Access Point.

MAC Address

Shows the MAC address of the managed Access Point.

Device Name

Displays the device name of the managed Access Point.

- When the AP is not a cluster member, click on this field and you'll be redirected to the configuration page where you can edit settings such as device name, IP Address, Wireless Radio settings.
- When the AP is a cluster member, click on this field to configure settings for individual Access Points by overriding the cluster settings.

IP Address

Shows the IP address of the managed Access Point.

Firmware Version

Shows the firmware version of the managed Access Point.

Last Update

Display the time the Access Point was last detected and the information was last updated.

Group

Displays the AP Group the Access Point is currently assigned to. Click on this field and you'll be redirected to the group configuration page.

Column Filter

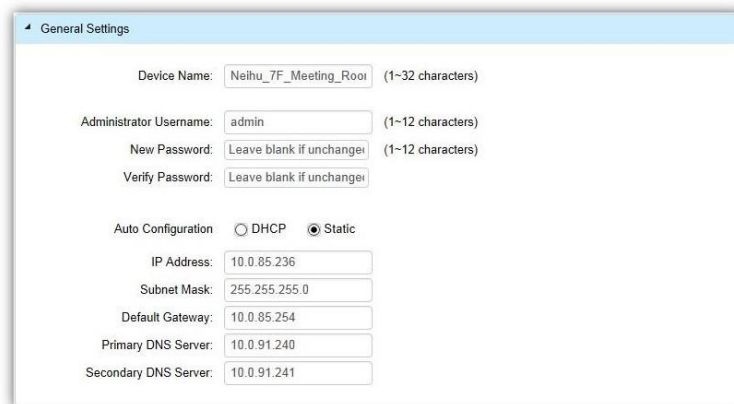
Shows or hides fields in the Access Point list.



Access Point Settings

On this page, you can edit the AP's name and password, manually assign an IP address, or change the channel selection, transmit power and other wireless settings of a managed Access Point.

General Settings



Device Name: The device name of the Access Point. Users can enter a custom name for the Access Point if they wish.

Administrator Username: Displays the current administrator login username for the Access Point. Enter a new Administrator username for the Access Point if you wish to change the username. The default username is: *admin*.

New Password: Enter a new password of between 1~12 alphanumeric characters.

Verify Password: Enter the password again for confirmation.

Auto Configuration: Select whether the device IP address will use the static IP address specified in the IP Address field or be obtained automatically when the device connects to a DHCP server.

IP Address: Enter the IP address for the Access Point.

Subnet Mask: Enter the Subnet Mask for the Access Point.

Default Gateway: Enter the default Gateway for the Access Point.

Primary/Secondary DNS Server: Enter the Primary/Secondary DNS server name.

Wireless Radio Settings

The screenshot shows a 'Wireless Radio Settings' window with a light blue header. Below the header, there are two main columns for '2.4GHz' and '5GHz' settings. At the top, a 'Country' dropdown is set to 'USA'. The '2.4GHz' column includes settings for 'Wireless Mode' (802.11 b/g/n Mixed), 'Channel HT Mode' (20MHz), 'Extension Channel' (Upper Channel), 'Channel' (Auto), 'Transmit Power' (19dBm), 'Client Limits' (126), 'Data Rate' (Auto), 'RTS/CTS Threshold' (2346), and 'Aggregation' (Enable). The '5GHz' column includes settings for 'Wireless Mode' (802.11 a/n Mixed), 'Channel HT Mode' (40MHz), 'Extension Channel' (Upper Channel), 'Channel' (Auto), 'Transmit Power' (18dBm), 'Client Limits' (126), 'Data Rate' (Auto), 'RTS/CTS Threshold' (2346), and 'Aggregation' (Enable). Both columns have a 'Frames (1~32)' and 'Bytes(Max) (2304~65535)' section at the bottom.

Country: Select a Country/Region to conform to local regulations. Different regions have different rules that govern which channels can be used for wireless communications.

Wireless Mode: Select from the drop-down menu to set the wireless mode for the Access Point. For 2.4GHz, the available options are 802.11b/g/n mixed, 802.11b, 802.11b/g mixed, 802.11g, and 802.11n. For 5GHz, the available options are 802.11a/n mixed, 802.11a, and 802.11n.

Channel HT Mode: Use the drop-down menu to select the Channel HT as 20MHz, 20/40MHz or 40MHz. A wider channel improves the performance, but some legacy devices operate only on either 20MHz or 40 MHz. This option is only available for 802.11n modes.

Extension Channel: Use the drop-down menu to set the Extension Channel as Upper or Lower channel. An extension channel is a secondary channel used to bond with the primary channel to increase this range to 40MHz allowing for greater bandwidth. This option is only available when Wireless Mode is 802.11n and Channel HT Mode is 20/40MHz or 40MHz.

Channel: Use the drop-down menu to select the wireless channel the radio will operate on. Optimizing channel assignments reduces channel interference and channel utilization for the network, thereby improving overall network performance and increasing the network's client capacity. The list of available channels that can be assigned to radios is determined based on which country the Access Points are deployed in.

Transmit Power: Allows you to manually set the transmit power on 2.4GHz or 5GHz radios. Increasing the power improves performance, but if two or more Access Points are operating in the same area on the same channel, it may cause interference.

Client Limits: Specify the maximum number of wireless clients that can associate with the radio. Enter a range from 1 to 127, or fill in 0 for an unlimited client limit.

Data Rate: Use the drop-down list to set the available transmit data rates permitted for wireless clients. The data rate affects the throughput of the access point. The lower the data rate, the lower the throughput, but the longer transmission distance.

RTS/CTS Threshold: Enter a Request to Send (RTS) Threshold value between 1~2346. Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same Access Point. Changing the RTS threshold can help control traffic flow through the Access Point. If you specify a lower threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the Access Point. Sending out more RTS packets can help the network recover from interference or collisions which might occur on a busy network or on a network experiencing electromagnetic interference.

Aggregation: Select whether to enable or disable Aggregation for the Access Point. This function merges data packets into one packet, reducing the number of packets. This also increases the packet sizes, so please keep this in mind. Aggregation is useful for increasing bandwidth throughput in environments that are prone to high error rates. This mode is only available for 802.11n modes. Fill in the frame rate limit you wish to use. The range is from 1~32. Next, fill in the max byte limit. The range is from 2304~65535.

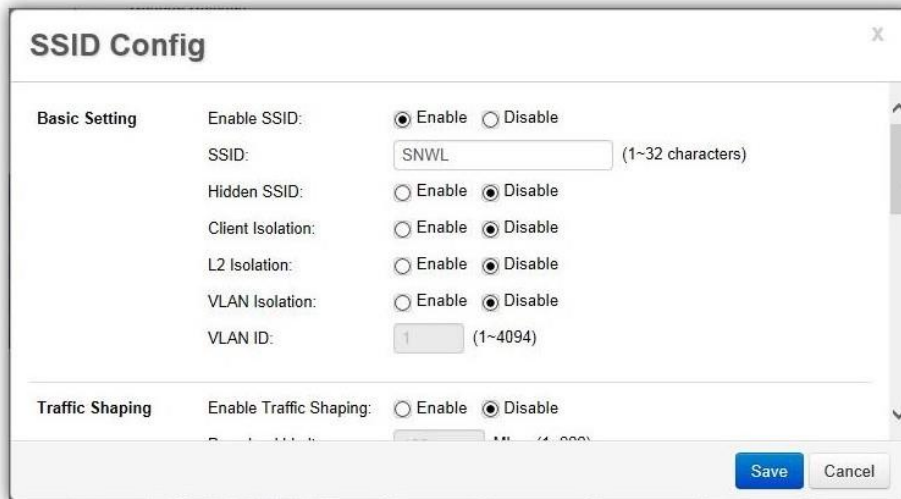
WLAN Settings - 2.4GHz/5GHz

Under the WLAN Settings, you can create and manage SSID configurations and profiles for the Access Points to fit your needs. An SSID is basically the name of the wireless network to which a wireless client can connect to. Multiple SSIDs allow administrators to use a single physical network to support multiple applications with different configuration requirements. Up to 8 SSIDs are available per radio. Click on the SSID you wish to make changes to and you'll be directed to the SSID Configuration page.

WLAN Settings - 2.4GHz									
ID	Status	SSID	Security	Encryption	Hidden SSID	Client Isolation	L2 Isolation	VLAN Isolation	VLAN ID
1	Enabled	SNWL	WPA2-PSK	AES	No	No	No	No	1
2	Disabled	210_2-2.4GHz	WPA2-PSK	AES	No	No	No	No	2
3	Disabled	SSID_3-2.4GHz	None	None	No	No	No	No	3
4	Disabled	SSID_4-2.4GHz	None	None	No	No	No	No	4
5	Disabled	SSID_5-2.4GHz	None	None	No	No	No	No	5
6	Disabled	SSID_6-2.4GHz	None	None	No	No	No	No	6
7	Disabled	SSID_7-2.4GHz	None	None	No	No	No	No	7
8	Disabled	SSID_8-2.4GHz	None	None	No	No	No	No	8

ID	The ID displays the SSID profile identifier.
Status	This displays whether the current SSID profile is enabled or disabled.
SSID	Displays the SSID name as it appears to the wireless clients in the network.
Security	Displays the security mode the SSID uses.
Encryption	Displays the data encryption type the SSID uses.
Hidden SSID	Displays whether the hidden SSID is enabled or disabled.
Client Isolation	Displays whether Client Isolation feature is enabled or disabled.
L2 Isolation	Displays whether L2 Isolation feature is enabled or disabled.
VLAN Isolation	Displays whether VLAN Isolation feature is enabled or disabled.
VLAN ID	<p>Displays the VLAN ID associated with the SSID.</p> <p>Note: For the Controller to function properly, make sure that all ports (on all cascading switches as well) connected to EWS APs on the switch are configured as the same VLAN ID as the Controller's Management VLAN ID.</p>

SSID Config



The screenshot shows the 'SSID Config' window with two tabs: 'Basic Setting' and 'Traffic Shaping'. The 'Basic Setting' tab is active and contains the following fields:

- Enable SSID:** Radio buttons for 'Enable' (selected) and 'Disable'.
- SSID:** Text input field containing 'SNWL' with a note '(1~32 characters)'.
- Hidden SSID:** Radio buttons for 'Enable' and 'Disable' (selected).
- Client Isolation:** Radio buttons for 'Enable' and 'Disable' (selected).
- L2 Isolation:** Radio buttons for 'Enable' and 'Disable' (selected).
- VLAN Isolation:** Radio buttons for 'Enable' and 'Disable' (selected).
- VLAN ID:** Text input field containing '1' with a note '(1~4094)'.

The 'Traffic Shaping' tab is partially visible below and contains the field:

- Enable Traffic Shaping:** Radio buttons for 'Enable' and 'Disable' (selected).

At the bottom right of the window are 'Save' and 'Cancel' buttons.

Enable SSID: Select to enable or disable the SSID broadcasting.

SSID: Enter the SSID for the current profile. This is the name that is visible to wireless clients on the network.

Hidden SSID: Enable this option if you do not want to broadcast this SSID. This can help to discourage wireless users from connecting to a particular SSID.

Client Isolation: When enabled, all communication between wireless clients connected to the same AP will be blocked.

L2 Isolation: When enabled, wireless client traffic from all hosts and clients on the same subnet will be blocked.

VLAN Isolation: When enabled, all communications between wireless clients and any other devices on different VLANs will be blocked. All frames from wireless clients connected to this SSID will be tagged a corresponded 802.1Q VLAN tag when going out from Ethernet port.

VLAN ID: Enter the VLAN ID for the SSID profile. The range is from 1~4094. When VLAN tagging is configured per SSID, all data traffic from wireless users associated to that SSID is tagged with the configured VLAN ID. Multiple SSIDs also can be configured to use the same VLAN tag. For instance, a single VLAN ID could be used to identify all wireless traffic traversing the network, regardless of the SSID. When the AP receives VLAN-tagged traffic from the upstream switch or router, it forwards that traffic to

the correct SSID. The AP drops all packets with VLAN IDs that are not associated to the SSID.

Traffic Shaping: Traffic Shaping regulates the allowed maximum downloading/uploading throughput per SSID. Select to enable or disable Wireless Traffic Shaping for the SSID.

- **Download Limit:** Specifies the allowed maximum throughput for downloading.
- **Upload Limit:** Specifies the allowed maximum throughput for uploading.

Fast Roaming: This feature uses protocols defined in 802.11r to allow continuous connectivity for wireless devices in motion, with fast and secure roaming from one AP to another. Coupled with 802.11k, wireless devices are able to quickly identify nearby APs that are available for roaming and once the signal strength of the current AP weakens and your device needs to roam to a new AP, it will already know which AP is the best to connect with. Note that not every wireless client supports 802.11k and 802.11r. Both the SSID and security options must be the same for this fast roaming to work. Fast Roaming is available when the following security methods are well configured:

WPA2-Enterprise	RADIUS server required
WPA-Mixed Enterprise	
WPA2-PSK	No RADIUS server required
WPA-Mixed	

Security: Select encryption method (WEP, WEP / WPA2 Enterprise, WPA-PSK / WPA2-PSK, or none) and encryption algorithm (AES or TKIP).

WEP: Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks which scrambles all data packets transmitted between the Access Point and the wireless clients associated with it. Both the Access Point and the wireless client must use the same WEP key for data encryption and decryption.

- **Mode:** Select Open System or Shared Key.
- **WEP Key:** Select the WEP Key you wish to use.
- **Input Type:** ASCII: Regular Text or HEX. Select the key type. Your available options are ASCII and HEX.

- **ASCII Key:** You can choose upper and lower case alphanumeric characters and special symbols such as @ and #.
- **HEX Key:** You can choose to use digits from 0~9 and letters from A~F. Select the bit-length of the encryption key to be used in the WEP connection. Your available options are: 64, 128, and 152-bit password lengths.
- **Key Length:** Select the desired option and ensure the wireless clients use the same setting. Your choices are: 64, 128, and 152-bit password lengths.
- **Key1/2/3/4:** Enter the Key value or values you wish to use.

WPA / WPA2 Enterprise: WPA and WPA2 are Wi-Fi Alliance IEEE 802.11i standards, which include AES and TKIP mechanisms.

- **Type:** Select the WPA type to use. Available options are Mixed, WPA and WPA2. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption:** Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).

Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.

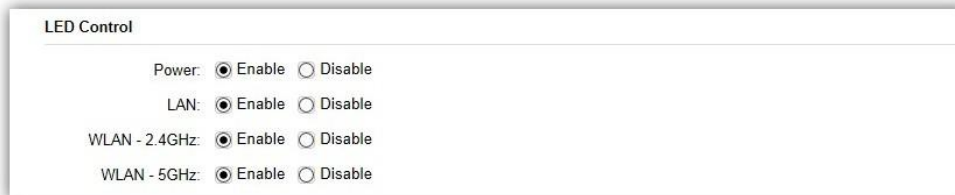
- **RADIUS Server:** Enter the IP address of the RADIUS server.
- **RADIUS Port:** Enter the port number used for connections to the RADIUS server.
- **RADIUS Secret:** Enter the secret required to connect to the Radius server.
- **Update Interval:** Specify how often, in seconds, the group key changes. Select 0 to disable.
- **RADIUS Accounting:** Enables or disables the accounting feature.
- **RADIUS Accounting Server:** Enter the IP address of the RADIUS accounting server.
- **RADIUS Accounting Port:** Enter the port number used for connections to the RADIUS accounting server.

- **RADIUS Accounting Secret:** Enter the secret required to connect to the RADIUS accounting server.
- **Accounting Group Key Update Interval:** Specify how often, in seconds, the accounting data sends. The range is from 60~600 seconds.

WPA-PSK / WPA2-PSK: WPA with PSK (Pre-shared key / Personal mode), designed for home and small office networks that don't require the complexity of an 802.1X authentication server.

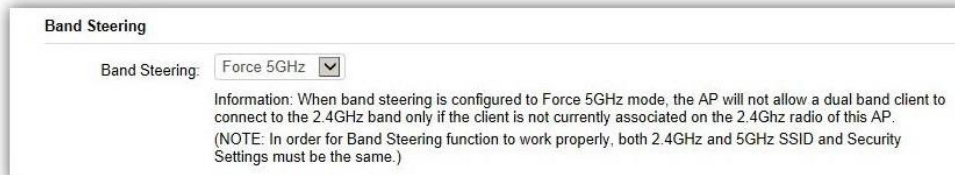
- **Type:** Select the WPA-PSK type to use. Available options are Mixed, WPA-PSK and WPA2-PSK. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption:** Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **WPA Passphrase:** Enter the Passphrase you wish to use. If you are using the ASCII format, the Key must be between 8~64 characters in length.
- **Group Key Update Interval:** Specify how often, in seconds, the Group Key changes.

Advanced Settings



LED Control	
Power:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LAN:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WLAN - 2.4GHz:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WLAN - 5GHz:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

LED Control: In some environments, the blinking LEDs on APs are not welcomed. This option allows you to enable or disable the devices LED indicators. Note that only indoor models support this feature.



Band Steering	
Band Steering:	Force 5GHz
<small>Information: When band steering is configured to Force 5GHz mode, the AP will not allow a dual band client to connect to the 2.4GHz band only if the client is not currently associated on the 2.4Ghz radio of this AP. (NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.)</small>	

Band Steering: When enabled, when the wireless client first associates with the AP, the AP will detect whether or not the wireless client is dual-band capable, and if it is, it will force the client to connect to the less congested 5GHz network to relieve congestion and overcrowding on the mainstream 2.4GHz frequency. It does this by actively blocking the client's attempts to associate with the 2.4GHz network. **Note: For Band Steering to take effect, both 2.4GHz and 5GHz SSIDs must have the same SSID and security settings. Wireless clients must be in both 2.4GHz and 5GHz wireless coverage zone when authenticating with the AP for the Band Steering algorithm to take effect.**

- **Prefer 5GHz:** All dual-band clients with 5GHz RSSI above the threshold will be connected to the 5GHz band.
- **Force 5GHz:** All dual-band clients will connect to the 5GHz.
- **Band Balance:** Automatically balances the number of newly connected clients across both 2.4GHz and 5GHz bands.

IMPORTANT INFORMATION: Band Steering only defines the action when a wireless client associates with an AP for the first time, and the wireless client must be in both 2.4GHz and 5GHz wireless coverage zone when authenticating with the AP for the Band Steering algorithm to take effect.

RSSI Threshold

Status: ☐ Enable ☒ Disable

RSSI: dBm (Range: -90dBm ~ -60dBm)

(NOTE: Enabling RSSI Threshold disassociates wireless clients that fall below the configured RSSI threshold and may cause wireless clients to reconnect frequently. It is recommended to disable this feature unless you deem it absolutely necessary.)

RSSI Threshold: With this feature enabled, in order to minimize the time the wireless client spends to passively scanning for a new AP to connect to, the AP will send a disassociation request to the wireless client upon detecting the wireless client's RSSI value lower than specified. The RSSI value can be adjusted to allow for more clients to stay associated to this Access Point. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently. It is recommended to disable this feature unless you deem it absolutely necessary.

Management VLAN

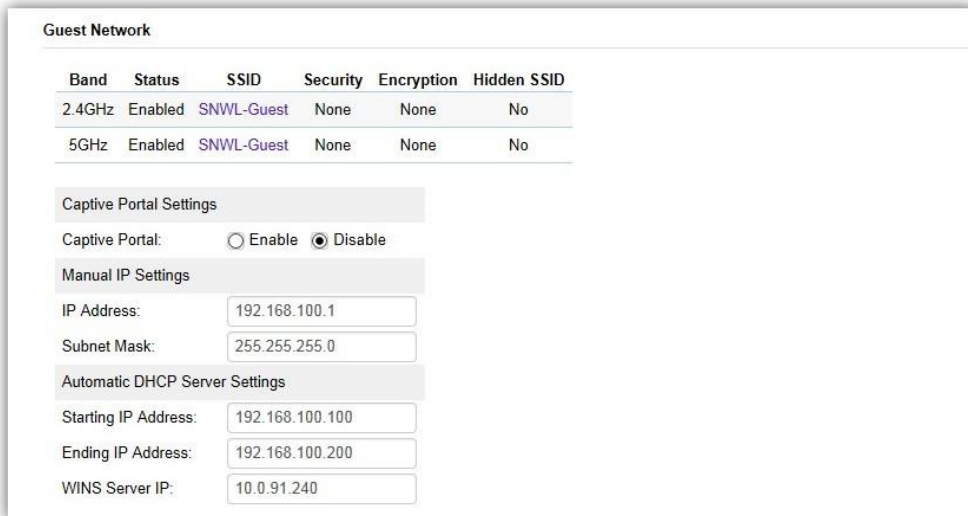
Status: ☐ Enable ☒ Disable

VLAN ID: (Range: 1 ~ 4094)

(WARNING: Enabling the management VLAN can cause the AP to lose connectivity with the controller. If you are utilizing the management VLAN, make sure that the controller and the AP are set to the same management VLAN to ensure proper connectivity.)

Management VLAN: Management VLAN can be used to separate management traffic from regular network traffic.

IMPORTANT INFORMATION: *When configuring or updating AP's Management VLAN settings, make sure that the same Management VLAN settings are applied to the ALL-WAPC0450C as well.*



Band	Status	SSID	Security	Encryption	Hidden SSID
2.4GHz	Enabled	SNWL-Guest	None	None	No
5GHz	Enabled	SNWL-Guest	None	None	No

Captive Portal Settings

Captive Portal: ☐ Enable ☒ Disable

Manual IP Settings

IP Address:

Subnet Mask:

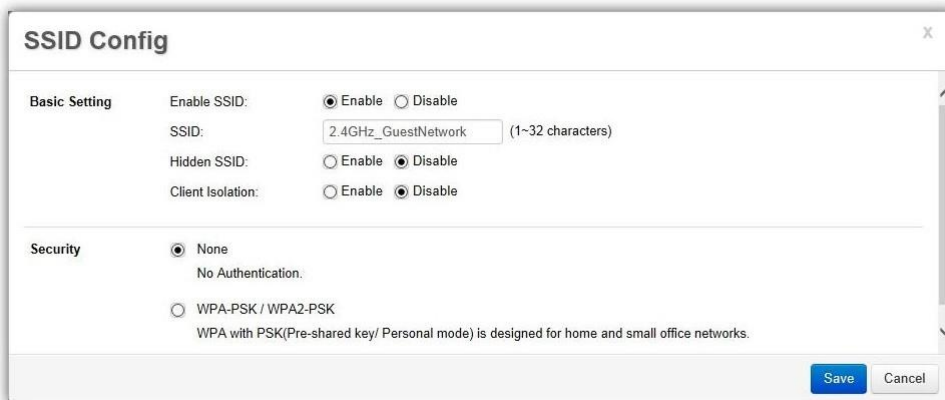
Automatic DHCP Server Settings

Starting IP Address:

Ending IP Address:

WINS Server IP:

Guest Network: The Guest Network feature allows administrators to grant Internet connectivity to visitors or guests while keeping other networking devices and sensitive personal or company information private and secure.



SSID Config

Basic Setting

Enable SSID: ☒ Enable ☐ Disable

SSID: (1~32 characters)

Hidden SSID: ☐ Enable ☒ Disable

Client Isolation: ☐ Enable ☒ Disable

Security

☒ None
No Authentication.

☐ WPA-PSK / WPA2-PSK
WPA with PSK(Pre-shared key/ Personal mode) is designed for home and small office networks.

Enable SSID: Select to enable or disable the SSID broadcasting.

SSID: Enter the SSID for the current profile. This is the name that is visible to wireless clients on the network.

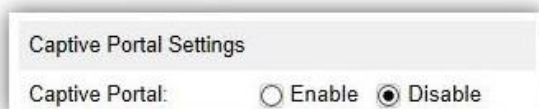
Hidden SSID: Enable this option if you do not want to broadcast this SSID. This can help to discourage wireless users from connecting to a particular SSID.

Client Isolation: When enabled, all communication between wireless clients connected to the same AP will be blocked.

Security: Select encryption method (WPA-PSK / WPA2-PSK, or none) and encryption algorithm (AES or TKIP).

WPA-PSK / WPA2-PSK: WPA with PSK (Pre-shared key / Personal mode), designed for home and small office networks that don't require the complexity of an 802.1X authentication server.

- **Type:** Select the WPA-PSK type to use. Available options are Mixed, WPA-PSK and WPA2-PSK. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption:** Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **WPA Passphrase:** Enter the Passphrase you wish to use. If you are using the ASCII format, the Key must be between 8~64 characters in length.
- **Group Key Update Interval:** Specify how often, in seconds, the Group Key changes.



Captive Portal: Select whether to Enable or Disable Captive Portal for Guest Network.

The screenshot shows a network configuration window with two sections. The first section, 'Manual IP Settings', contains two input fields: 'IP Address' with the value '192.168.100.1' and 'Subnet Mask' with the value '255.255.255.0'. The second section, 'Automatic DHCP Server Settings', contains three input fields: 'Starting IP Address' with the value '192.168.100.100', 'Ending IP Address' with the value '192.168.100.200', and 'WINS Server IP' with the value '0.0.0.0'.

Manual IP Settings	
IP Address:	192.168.100.1
Subnet Mask:	255.255.255.0

Automatic DHCP Server Settings	
Starting IP Address:	192.168.100.100
Ending IP Address:	192.168.100.200
WINS Server IP:	0.0.0.0

Manual IP Settings

- **IP Address:** Enter the IP address for the default gateway of clients associated to the Guest Network.
- **Subnet Mask:** Enter the Subnet mask for the Guest Network.

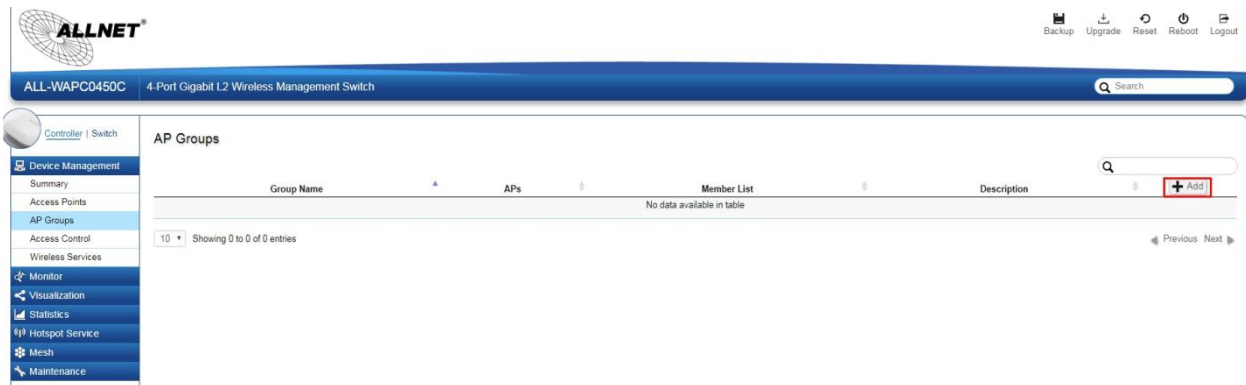
Automatic DHCP Server Settings

- **Starting IP Address/Ending IP Address:** Enter the pool range of IP addresses available for assignment.
- **WINS Server IP:** Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

After settings are changed, click **Apply** to save the changes to the system.

AP Groups

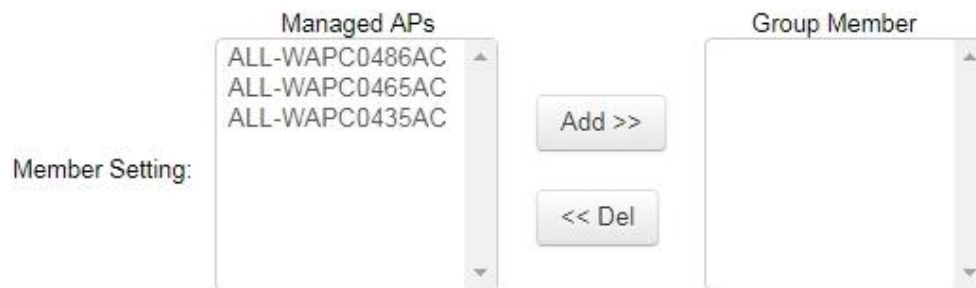
An AP Group can be used to define configuration options and apply them to a number of APs at once. If your wireless network covers a large physical environment and you want to provide wireless services with different settings and policies to different areas of your environment, you can use AP Groups to do this instead of having to modify the settings of each AP individually. For example, if your wireless network covers two floors and you need to provide wireless access to visitors on the 1st Floor, you can simply setup two different AP Groups with different settings and policies to suit your application.



Creating a New AP Group

Follow the steps below to create a new AP Group.

1. Click on **Add** button to create a new AP Group.



2. Enter the name and description of the new AP Group.

3. In the Member Setting section, all Access Points that are managed by the ALL-WAPC0450C that are not currently assigned to an AP Group will be listed on the left. Select the Access Points you wish to assign to this group and press **Add**. The Access Points will be moved to the right column.
4. Configure Radio, WLAN, and Advanced settings then click on Apply for settings to take effect.

Search Bar

Use the Search Bar to search for keywords in the list using the following criteria: AP Group Name, AP MAC, AP Name, Description.



Add Button

Use the Add Button to create a new AP Group.



Edit Button

Use the Edit Button to edit the configurations of the AP Group.



Delete Button

Use the Delete Button to remove an AP Group.



Access Control

This page displays the list of wireless clients previously blocked from your network. If for any reason, you need to block a client device from your network, you can do so from this page by creating a new rule and entering the client's MAC address.

Blocking a Specific Client Device

Follow the steps below to permanently block a specific client device from the network.

1. Click the **Add** button to create a new block rule.
2. Enter the *MAC Address* and *Description* of the wireless client device you wish to block.
3. Click on **Apply** to create a new rule.
4. Click on the **Apply** button on the upper right to save settings made on this page.

Unblocking a Previously Blocked Client Device

1. Click on the **Delete** button on the client device you wish to unblock.
2. Click on the **Apply** button on the upper right to save settings made on this page.



Blocked Clients

Displays the total number of clients permanently blocked from the network.



Apply Button

Click on Apply to save changes made on this page.



Search Bar

Use the Search Bar to search for blocked clients in the list using the following criteria:
Client MAC Address, Description.



Add Button

Use the Add Button to add a new block rule.



Edit Button

Use the Edit Button to edit the Client MAC Address or Description of the rule.



Delete Button

Use the Delete Button to remove the rule.



Wireless Services

ALLNET®

ALL-WAPC0450C 4-Port Gigabit L2 Wireless Management Switch

Controller | Switch

Device Management

- Summary
- Access Points
- AP Groups
- Access Control
- Wireless Services

Monitor

Visualization

Statistics

Hotspot Service

Mesh

Maintenance

Service Settings

Background Scanning

- ☒ Enable background scanning on 2.4GHz radio every 1000 seconds. (10 ~ 1000)
- ☒ Enable background scanning on 5GHz radio every 1000 seconds. (10 ~ 1000)

Auto TX Power

- ☒ Enable Auto TX Power on 2.4GHz radio
- ☒ Enable Auto TX Power on 5GHz radio

Apply

Background Scanning

With Background Scanning enabled, the controller periodically samples RF activity of all Access Points including channel utilization and surrounding devices in all available channels. Background scanning is the basis of Auto Channel, Auto Tx Power and Rogue AP detection, and must be enabled for these features to operate. You may, if you prefer, disable it if you feel it's not helpful, or adjust the scanning frequency, if you want scans at greater or fewer intervals.

Note: For latency-sensitive applications such as VoIP, it is recommended to set the background scan interval to a higher value, e.g. 5 or 10 minutes. For regular application, the recommended value is 30 seconds. This value will also be directly related on how long it takes for the AP to scan for rogue devices.

Auto TX Power

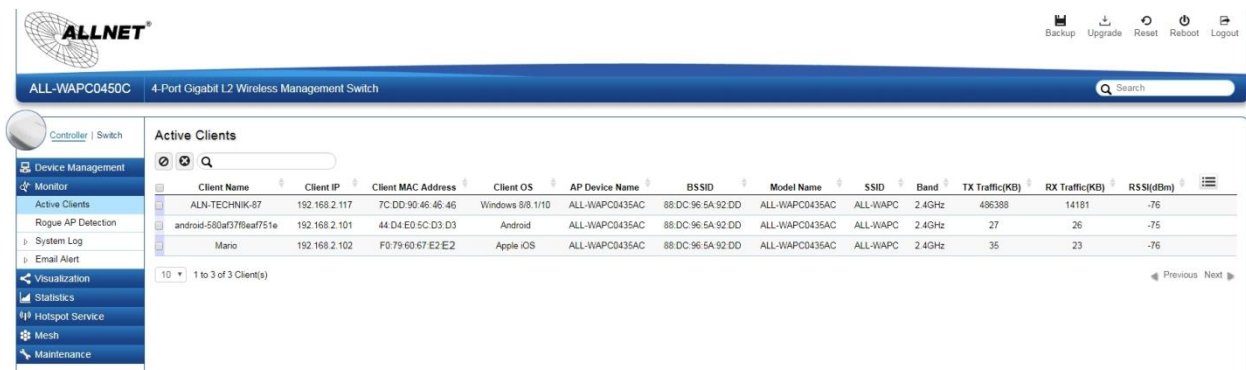
Using the information collected by Background Scanning, APs can automatically adjust their transmit power to optimize coverage. When enabled, APs will optimize their transmit power based on the time interval configured for Background Scanning.

Note: Background Scanning must be **enabled** and Tx Power of APs must be set to **Auto** (under Wireless Radio Settings) for this feature to operate.

Monitor

Active Clients

From here, you can view information, temporarily disconnect and permanently block the wireless clients that are associated with the Access Points that the ALL-WAPC0450C manages. The ALL-WAPC0450C is able to identify client devices by their Operating System, device type and host name, if available. If multiple Access Points are connected to the network, use the search bar to find an Access Point by its name.



Client Name	Client IP	Client MAC Address	Client OS	AP Device Name	BSSID	Model Name	SSID	Band	TX Traffic(KB)	RX Traffic(KB)	RSSI(dBm)
ALN-TECHNIK-87	192.168.2.117	7C-DD-90-46-46-46	Windows 8/8.1/10	ALL-WAPC0435AC	88-DC-96-5A-92-DD	ALL-WAPC0435AC	ALL-WAPC	2.4GHz	486388	14181	-76
android-580ar378ear751e	192.168.2.101	44-D4-E0-5C-D3-D3	Android	ALL-WAPC0435AC	88-DC-96-5A-92-DD	ALL-WAPC0435AC	ALL-WAPC	2.4GHz	27	26	-75
Mario	192.168.2.102	F0-79-60-67-E2-E2	Apple iOS	ALL-WAPC0435AC	88-DC-96-5A-92-DD	ALL-WAPC0435AC	ALL-WAPC	2.4GHz	35	23	-76

Kick Client

Use this function to temporarily disconnect a wireless client from the network. The disconnected client can simply reconnect manually if they wish to.



Ban Client

Use this function to permanently block a wireless client from the network. Go to **Device Management > Access Control** to



unblock the wireless client.

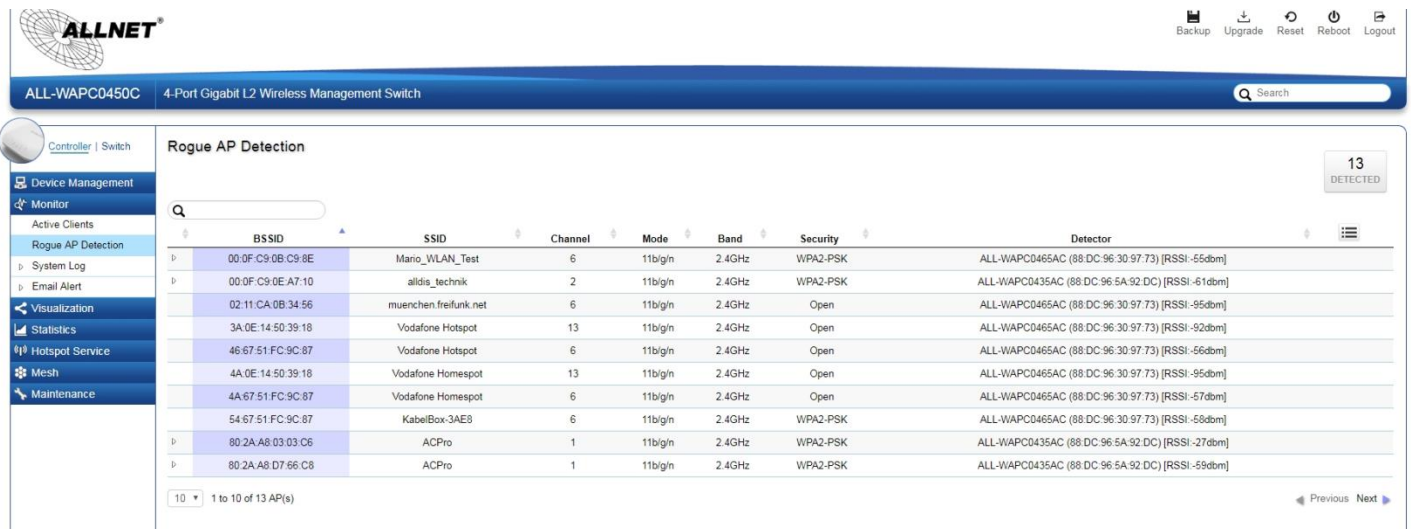
Search Bar

Use the Search Bar to search for Wireless Clients managed by the ALL-WAPC0450C using the following criteria: Client Name, Client IP, Client MAC Address, Client OS, AP Device Name, AP MAC Address, Model Name, SSID, Band, TX Traffic, RX Traffic.

Client Name	Displays the name of the wireless client connected to the Access Point.
Client IP	Displays the IP address of the wireless client connected to the Access Point.
Client MAC Address	Displays the MAC address of the wireless client connected to the Access Point.
Client OS	Displays the type of operating system the wireless client connected to the Access Point is running on.
AP Device Name	Displays the name of the Access Point which the client is connected to.
AP MAC Address	Displays the MAC address of the Access Point which the client is connected to.
Model Name	Displays the model name of the Access Point which the client is connected to.
SSID	Displays the SSID of the Access Point which the client is connected to.
Band	Displays whether the wireless client is connected to the 2.4GHz or 5GHz radio.
TX Traffic (KB)	Displays the total traffic transmitted to the Wireless Client.
RX Traffic (KB)	Displays the total traffic received from the Wireless Client.
RSSI (dBm)	Displays the received signal strength indicator in terms of dBm.

Rogue AP Detection

Rogue Access Points refer to those unauthorized and often unmanaged APs attached to an existing wired network which could bring harm to the network or may be used to deliberately gain access to confidential company information. With **Background Scanning** enabled, the Rogue AP Detection feature can be used to periodically scan 2.4 GHz and 5 GHz frequency bands to identify rogue wireless Access Points not managed by the ALL-WAPC0450C.



The screenshot shows the ALLNET web interface for the ALL-WAPC0450C 4-Port Gigabit L2 Wireless Management Switch. The 'Rogue AP Detection' page is active, displaying a table of detected rogue access points. The table has columns for BSSID, SSID, Channel, Mode, Band, Security, and Detector. A search bar is located at the top of the table. The interface also includes a sidebar with navigation options like Device Management, Monitor, Active Clients, and Rogue AP Detection.

BSSID	SSID	Channel	Mode	Band	Security	Detector
00:0F:C9:0B:C9:8E	Mario_WLAN_Test	6	11b/g/n	2.4GHz	WPA2-PSK	ALL-WAPC0465AC (88:DC:96:30:97:73) [RSSI: -55dbm]
00:0F:C9:0E:A7:10	alidis_techink	2	11b/g/n	2.4GHz	WPA2-PSK	ALL-WAPC0435AC (88:DC:96:5A:92:DC) [RSSI: -61dbm]
02:11:CA:0B:34:56	muenchen.freifunk.net	6	11b/g/n	2.4GHz	Open	ALL-WAPC0465AC (88:DC:96:30:97:73) [RSSI: -95dbm]
3A:0E:14:50:39:18	Vodafone Hotspot	13	11b/g/n	2.4GHz	Open	ALL-WAPC0465AC (88:DC:96:30:97:73) [RSSI: -92dbm]
46:67:51:FC:9C:87	Vodafone Hotspot	6	11b/g/n	2.4GHz	Open	ALL-WAPC0465AC (88:DC:96:30:97:73) [RSSI: -56dbm]
4A:0E:14:50:39:18	Vodafone Homespot	13	11b/g/n	2.4GHz	Open	ALL-WAPC0465AC (88:DC:96:30:97:73) [RSSI: -95dbm]
4A:67:51:FC:9C:87	Vodafone Homespot	6	11b/g/n	2.4GHz	Open	ALL-WAPC0465AC (88:DC:96:30:97:73) [RSSI: -57dbm]
54:67:51:FC:9C:87	KabelBox-3AE8	6	11b/g/n	2.4GHz	WPA2-PSK	ALL-WAPC0465AC (88:DC:96:30:97:73) [RSSI: -58dbm]
80:2A:A8:03:03:C6	ACPro	1	11b/g/n	2.4GHz	WPA2-PSK	ALL-WAPC0435AC (88:DC:96:5A:92:DC) [RSSI: -27dbm]
80:2A:A8:D7:66:C8	ACPro	1	11b/g/n	2.4GHz	WPA2-PSK	ALL-WAPC0435AC (88:DC:96:5A:92:DC) [RSSI: -59dbm]

Search Bar

Use the Search Bar to search for Rogue Access Points detected using the following criteria: BSSID, SSID, Type, Channel, Mode, Band, Security, Detector.



BSSID	Displays the BSSID of the rogue device detected.
SSID	Displays the SSID of the rogue device detected.

Type	Displays the type of the rogue device detected.
Channel	Displays the channel of the rogue device detected.
Mode	Displays the wireless mode of the rogue device detected.
Band	Displays the band of the rogue device detected.
Security	Displays the encryption method of the rogue device detected.
Detector	Displays the name and MAC address of the managed AP which detected the rogue device.

Column Filter

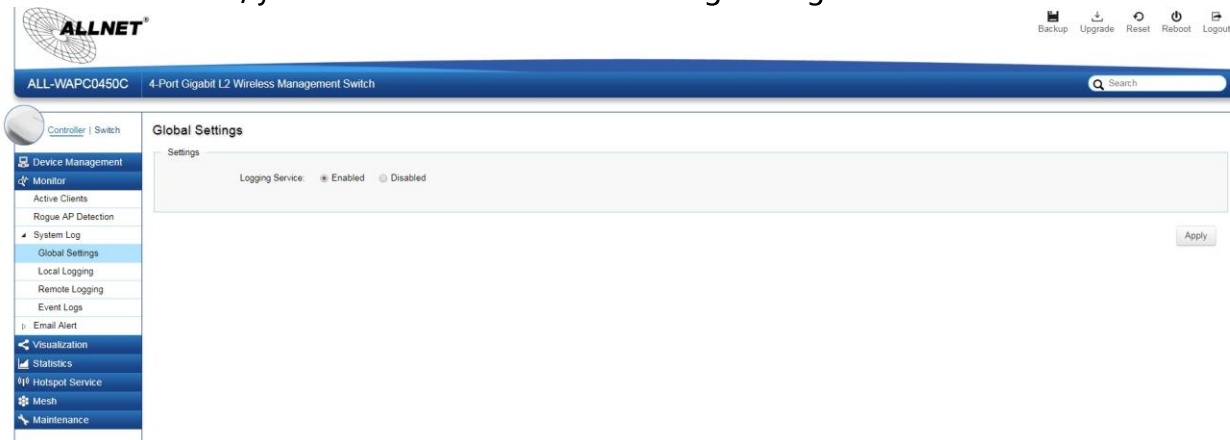
Shows or hides fields in the list.



System Log

Global Settings

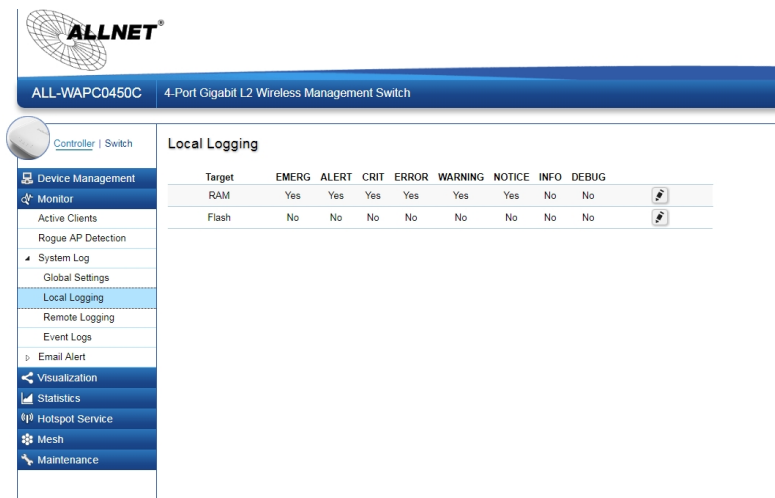
From here, you can Enable or Disable the Log settings for the ALL-WAPC0450C.



Local Logging

The System Log is designed to monitor the operation of the ALL-WAPC0450C by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

The ALL-WAPC0450C supports log output to two directions: Flash and RAM. The information stored in the system's RAM log will be lost after the Switch is rebooted or powered off, whereas the information stored in the system's Flash will be kept effective even if the Switch is rebooted or powered off. The log has a fixed capacity; at a certain level, the ALL-WAPC0450C will start deleting the oldest entries to make room for the newest.



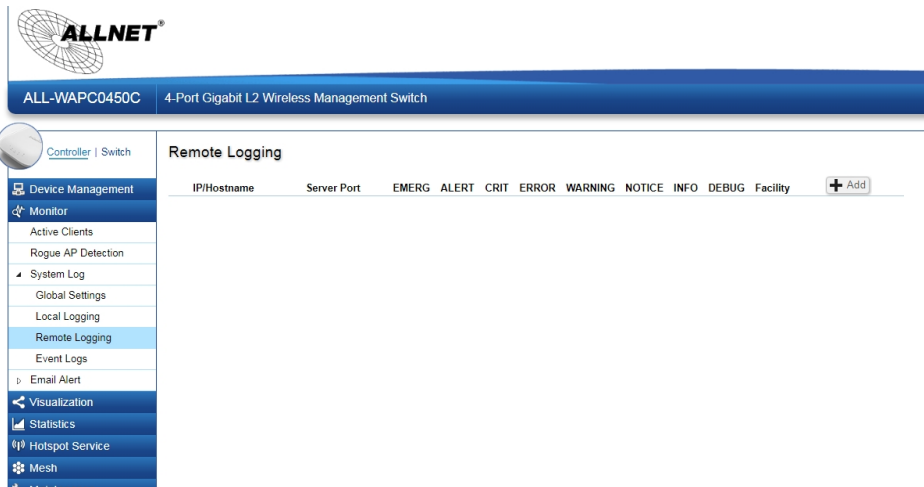
Severity Level

RFC 5424 defines eight severity levels:

Code	Severity	Description	General Description
0	EMERG	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	ALERT	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	CRIT	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	ERROR	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	WARNING	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	NOTICE	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	INFO	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.

Remote Logging

The internal log of the ALL-WAPC0450C has a fixed capacity; at a certain level, the ALL-WAPC0450C will start deleting the oldest entries to make room for the newest. If you want a permanent record of all logging activities, you can set up your syslog server to receive log contents from the ALL-WAPC0450C. Use this page to direct all logging to the syslog server. Click the Add button, define your syslog server, and select the severity level of events you wish to log.



IP/Hostname

Specify the IP address or host name of syslog server.

Server Port

Specify the port of the syslog server. The default port is 514.

Severity Level

RFC 5424 defines eight severity levels:

Code	Severity	Description	General Description
0	EMERG	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	ALERT	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	CRIT	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	ERROR	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.


4	WARNING	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	NOTICE	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	INFO	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.

Facility

The log facility is used to separate out log messages by application or by function, allowing you to send logs to different files in the syslog server. Use the drop-down menu to select local0, local1, local2, local3, local4, local5, local6, or local7.

Event Logs

This page displays the most recent records in the ALL-WAPC0450C's internal log. Log entries are listed in reverse chronological order (with the latest logs at the top of the list). Click a column header to sort the contents by that category.



ALL-WAPC0450C 4-Port Gigabit L2 Wireless Management Switch

Controller | Switch

- Device Management
- Monitor
 - Active Clients
 - Rogue AP Detection
 - System Log
 - Global Settings
 - Local Logging
 - Remote Logging
 - Event Logs
 - Email Alert
- Visualization
- Statistics
- Hotspot Service
- Mesh
- Maintenance

Event Logs

Display logs in: RAM

Time	Category	Severity	Message
Oct 12 2017 17:00:21	AAA	notice	New http connection for user admin, source 192.168.2.7 ACCEPTED
Oct 12 2017 16:48:31	AAA	notice	New http connection for user admin, source 192.168.2.7 ACCEPTED
Oct 12 2017 13:46:53	AAA	notice	New http connection for user admin, source 192.168.2.7 ACCEPTED
Oct 12 2017 11:44:16	AAA	notice	New http connection for user admin, source 192.168.2.7 ACCEPTED
Oct 12 2017 09:52:25	AAA	notice	New http connection for user admin, source 192.168.2.7 ACCEPTED
Oct 12 2017 09:33:22	AAA	notice	New http connection for user admin, source 192.168.2.10 ACCEPTED
Oct 12 2017 09:01:19	AAA	notice	New http connection for user admin, source 192.168.2.10 ACCEPTED
Oct 12 2017 08:43:20	AAA	notice	New http connection for user admin, source 192.168.2.7 ACCEPTED
Oct 12 2017 08:40:51	AAA	notice	New http connection for user admin, source 192.168.2.7 ACCEPTED
Jan 01 2000 01:01:14	AP	warning	ALL-WAPC0465AC(88:DC:96:30:97:73) has invalid IP(192.168.2.115)

10 1 to 10 of 16 event(s)

Display logs in

- **RAM:** The information stored in the system's RAM log will be lost after the Switch is rebooted or powered off
- **Flash:** The information stored in the system's Flash will be kept effective even if the Switch is rebooted or powered off.

Type:

- **Controller:** Display controller related logs.
- **Switch:** Display switch related logs.
- **All:** Display logs for both controller and switch.

Export

Click Export button to export the current buffered log to a .txt file.

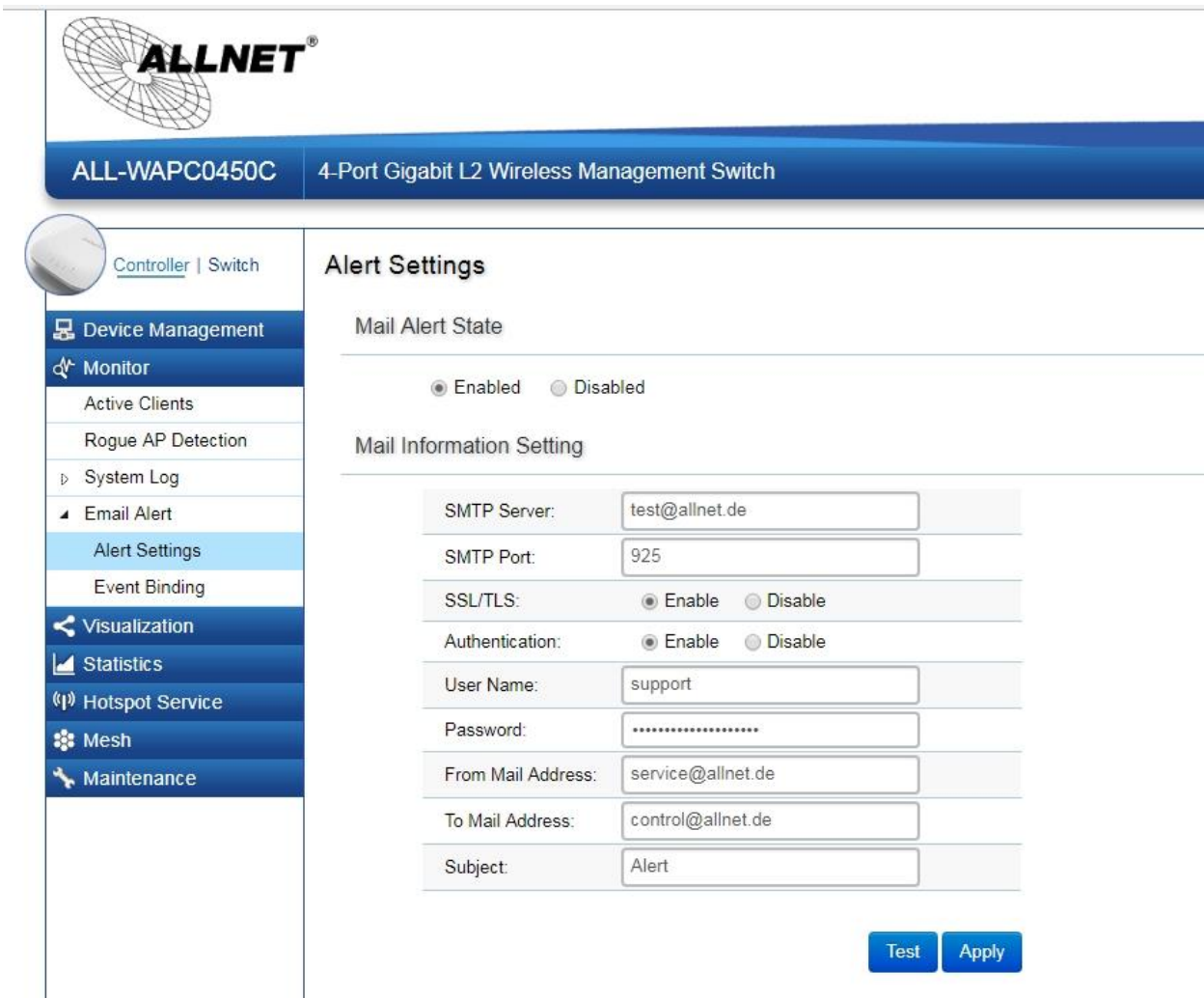
Clear

Click Clear button to clear the buffered log in the system's memory.

Email Alert

Alert Settings

If an alert is detected, the ALL-WAPC0450C will record it in the event log. The ALL-WAPC0450C can also be configured to send email notifications for selected events.



The screenshot shows the web interface of the ALLNET 4-Port Gigabit L2 Wireless Management Switch. The top header features the ALLNET logo and the device name. A left sidebar contains navigation menus for Device Management, Monitor, System Log, Email Alert, Visualization, Statistics, Hotspot Service, Mesh, and Maintenance. The main content area is titled 'Alert Settings' and includes sections for 'Mail Alert State' and 'Mail Information Setting'. The 'Mail Alert State' section has radio buttons for 'Enabled' (selected) and 'Disabled'. The 'Mail Information Setting' section contains input fields for SMTP Server, SMTP Port, SSL/TLS, Authentication, User Name, Password, From Mail Address, To Mail Address, and Subject. At the bottom right, there are 'Test' and 'Apply' buttons.

ALL-WAPC0450C		4-Port Gigabit L2 Wireless Management Switch	
Alert Settings			
Mail Alert State			
<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled			
Mail Information Setting			
SMTP Server:	test@allnet.de		
SMTP Port:	925		
SSL/TLS:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Authentication:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
User Name:	support		
Password:	*****		
From Mail Address:	service@allnet.de		
To Mail Address:	control@allnet.de		
Subject:	Alert		
<input type="button" value="Test"/> <input type="button" value="Apply"/>			

Mail Alert State: Select whether to Enable/Disable email notification.

Mail Information Setting

- **SMTP Server:** Enter the name of the mail server.
- **SMTP Port:** Enter the SMTP port.
- **SSL/TSL:** Enable this option if your mail server uses SSL/TLS encryption.

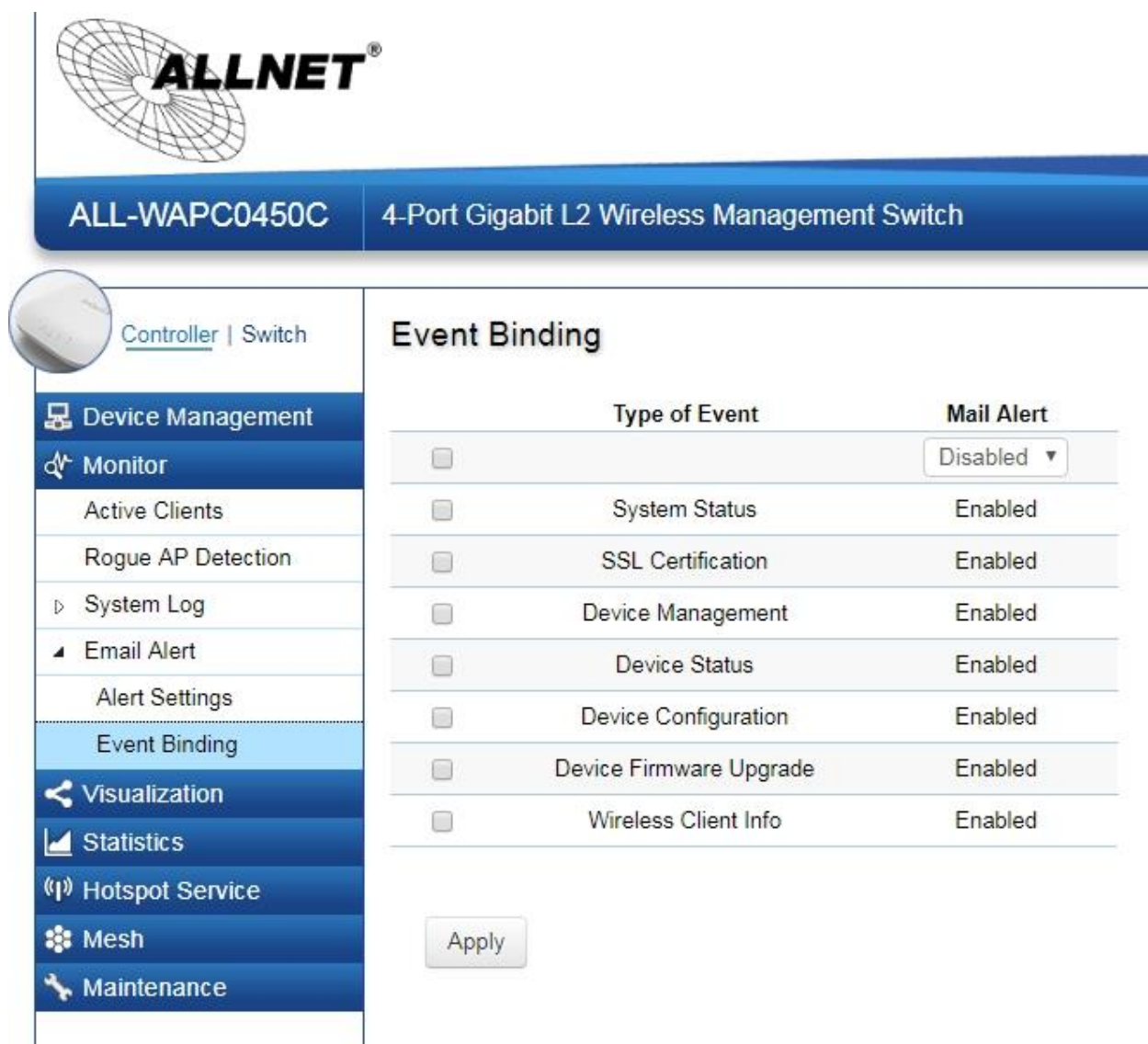
- **Authentication:** Select this option to enable authentication.
- **User Name:** Enter the username required by the mail server.
- **Password:** Enter the password required by the mail server.
- **From Mail Address:** Enter the email address that will appear as the sender of the email alert.
- **To Mail Address:** Enter the email address which the ALL-WAPC0450C will send alarm messages to. You can only send alarm messages to a single email address.
- **Subject:** Enter the subject of the email notification.

Test: To verify that the ALL-WAPC0450C can send email notifications using the SMTP settings you configured, click the **Test** button.

Apply: Click **Apply** to save settings.

Event Binding

Use this page to choose which types of events will trigger the ALL-WAPC0450C to send an email notification. When any of the selected events occur, the ALL-WAPC0450C sends an email notification to the email address that you specified in the **Monitoring > Email Alert > Alert Settings** section.



ALLNET
ALL-WAPC0450C 4-Port Gigabit L2 Wireless Management Switch

Controller | Switch

- Device Management
- Monitor
 - Active Clients
 - Rogue AP Detection
 - System Log
 - Email Alert
 - Alert Settings
 - Event Binding**
- Visualization
- Statistics
- Hotspot Service
- Mesh
- Maintenance

Event Binding

Type of Event	Mail Alert
<input type="checkbox"/>	Disabled ▼
<input type="checkbox"/> System Status	Enabled
<input type="checkbox"/> SSL Certification	Enabled
<input type="checkbox"/> Device Management	Enabled
<input type="checkbox"/> Device Status	Enabled
<input type="checkbox"/> Device Configuration	Enabled
<input type="checkbox"/> Device Firmware Upgrade	Enabled
<input type="checkbox"/> Wireless Client Info	Enabled

Apply

The table below provides explanations for EWS Controller syslog event messages.

Event Type	EWS Syslog Message	Severity Level
Status of AP Controller	Controller is enabled	INFO
Status of AP Controller	Controller is disabled	WARNING

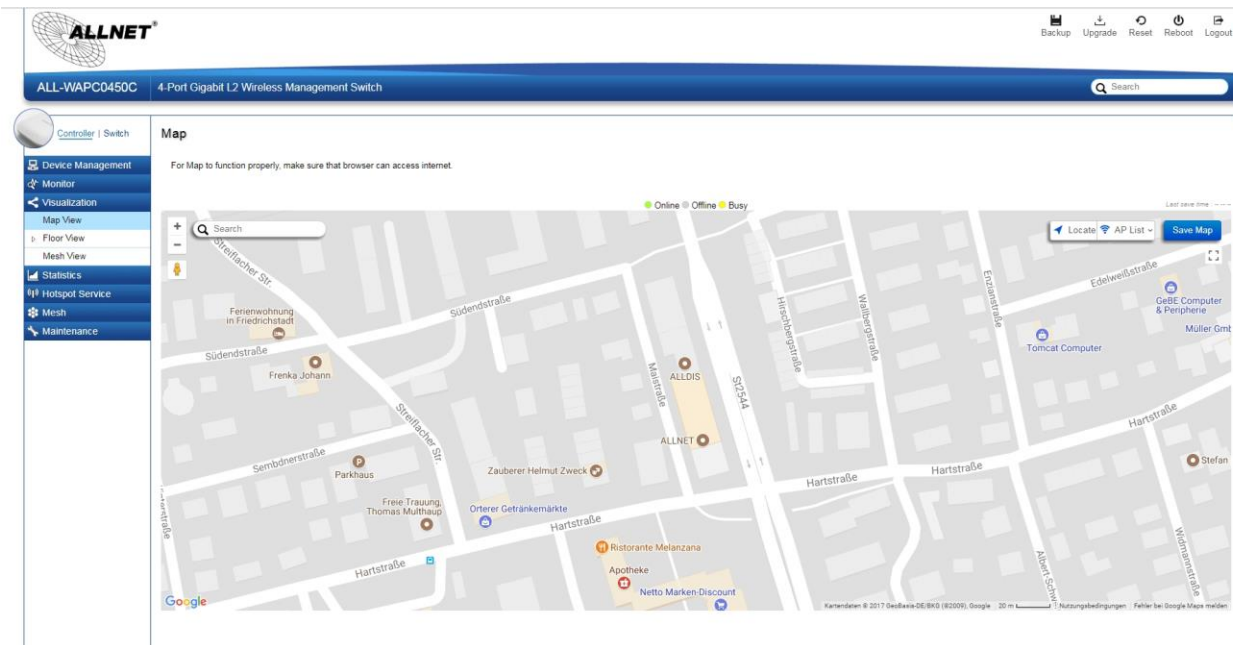
Certificate Changed	SSL certificate updated	INFO
Certificate Changed	SSL certificate will expire in {value} days	WARNING
Certificate Changed	SSL certificate has expired	ERROR
Certificate Changed	[AP Name] [AP MAC]'s SSL certificate has been updated	INFO
AP Managed	[AP Name] [AP MAC] added to management list	INFO
AP Managed	[AP Name] [AP IP] removed from management list	INFO
Status of AP	[AP Name] [AP MAC] online	INFO
Status of AP	[AP Name] [AP MAC] reset	INFO

Status of AP	[AP Name] [AP MAC] offline	WARNING
Status of AP	[AP Name] [AP MAC] has invalid IP [IP Address]	WARNING
Status of AP	[AP Name] [AP MAC]'s active client number reaches client limits {value} of [2.4/5]GHz	WARNING
AP Configuration Changed	[AP Name] [AP MAC] configuration updated	INFO
AP Firmware	[AP Name] [AP MAC] firmware version is incompatible	WARNING
AP Firmware	[AP Name] [AP MAC] started to upgrade firmware from [old-ver] to [new-ver]	INFO
AP Firmware	[AP Name] [AP MAC] firmware upgrade failed	ERROR

Map View


From here, you can view a geographical representation of Access Points in the network. Click AP List to display the list of Access Points managed by the ALL-WAPC0450C then simply click-and-drag the AP marker to the desired location on the map.

Note: Your browser needs to be able to access the Internet for this function to work.



AP Status	Description
Online	The managed AP is currently online
Offline	The managed AP is currently offline
Busy	The managed AP is currently busy (applying new configuration settings)

Navigating Tips

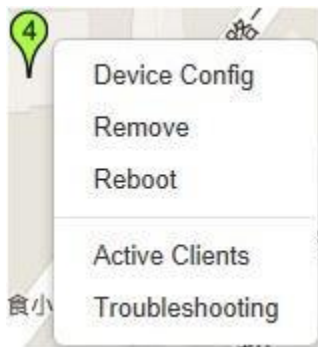
Use  to scroll up, down, left, or right.

Use the slider bar to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.



Use the **Search box** to search for locations by typing an address or the name of a landmark.

Use the **Locate** button to pinpoint the map to your current location. Note that the location provided is calculated based on your IP address and results might be inaccurate.



Left click on the Access Point marker to bring up a menu where you can configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

Click on [Save Map](#) for the settings to take effect.

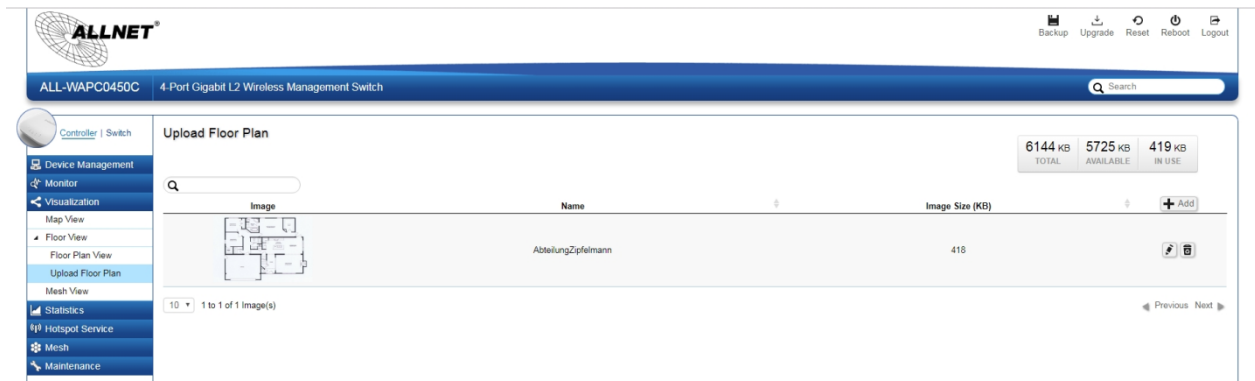
Floor View

The Floor View feature enables an administrator to upload custom floor plans and place AP markers in relevant locations for better network visualization of a wireless network. Multiple images can be uploaded to visualize Access Point placement on multiple floors of an office building or different branch offices within an organization.

Floorplan Image

From here, an administrator can add or delete a custom map or floor plan image. An unlimited number of floor plan images can be imported to the ALL-WAPC0450C. However, the total

file size of all imported floor plans is limited to 6MB and the maximum file size per image is 512KB (a smaller image loads faster). Valid image file formats are .PNG, .GIF or .JPG.



Status Dashboard

Total: Displays the total memory storage space allocated for uploading custom floor plans.

Available: Display the memory storage space that is currently available.

In Use: Displays the memory storage space that is currently in use.

6144 KB	6056 KB	88 KB
TOTAL	AVAILABLE	IN USE

Add Button

Use the Add Button to import a new image.



Edit Button

Use the Edit Button to edit the Name/Description of the imported image.



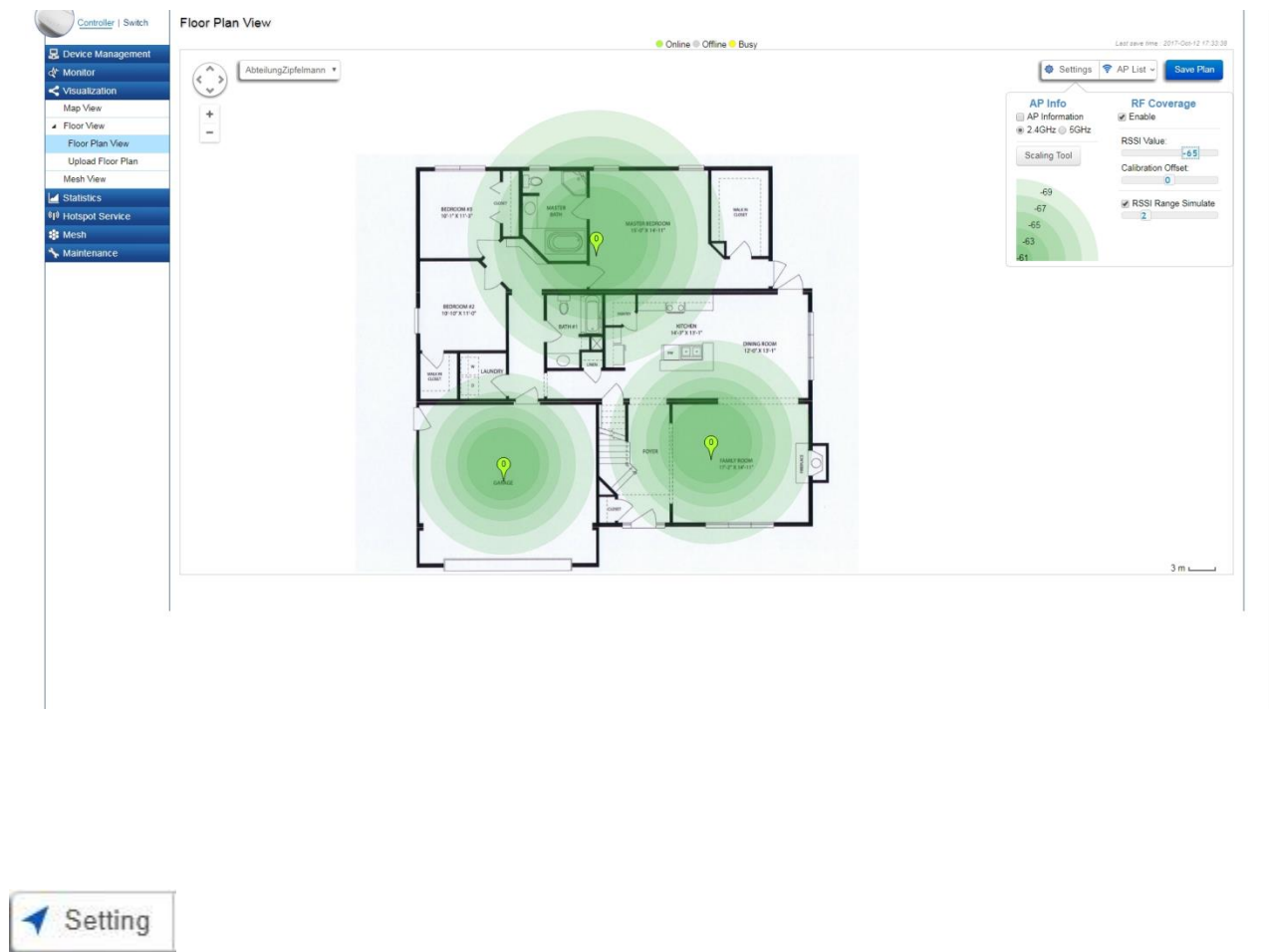
Delete Button

Use the Delete Button to remove the image.



Floorplan View

After importing your floor plan image, you can distribute markers that represent the APs to the correct locations by clicking on **AP List** and dragging each marker icon to its correct location on the floor plan. Also, Wireless Coverage Display can be toggled on to indicate the coverage range of each AP, assisting IT managers to easily and accurately plan and deploy wireless networks in any indoor environment. Click on **Save Plan** when you're done to save settings.



Settings

Last save time : 2017-Oct-12 17:33:38

Settings

AP List ▾

Save Plan

AP Info

☐ AP Information

☒ 2.4GHz ☐ 5GHz

Scaling Tool



RF Coverage

☒ Enable

RSSI Value:

Calibration Offset:

☒ RSSI Range Simulate

AP Info

AP Information: Select to toggle on/off AP detailed information to be shown on your floor plan.

2.4 GHz / 5GHz: Select whether to display signal coverage of 2.4GHz or 5GHz radio. The wireless coverage displayed will be based on the transmit power settings of the Access Point.

Scaling Tool: Use the scaling tool to determine the exact distance on the floorplan.

Signal Indicator: The colored indicator displays the reference signal strength covered.

RF Coverage


Enable: Select to display wireless coverage on your floor plan.


RSSI Value: Adjust RSSI value to emulate using the slider bar.

Calibration Offset: Use the slider bar to adjust the offset value based on the deployment.

RSSI Range Simulate: Check the **RSSI Simulate** box to display RSSI reference on your floor plan. Adjust RSSI coverage range to emulate using the slider bar.

Navigating Tips

Use  to scroll up, down, left, or right.

Use  to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Mouse over a device to show information about the device.




AP List: Click to reveal a list of APs that the ALL-WAPC0450C is currently managing.

The number in the marker represents the number of wireless clients that are currently connected to the Access Point.



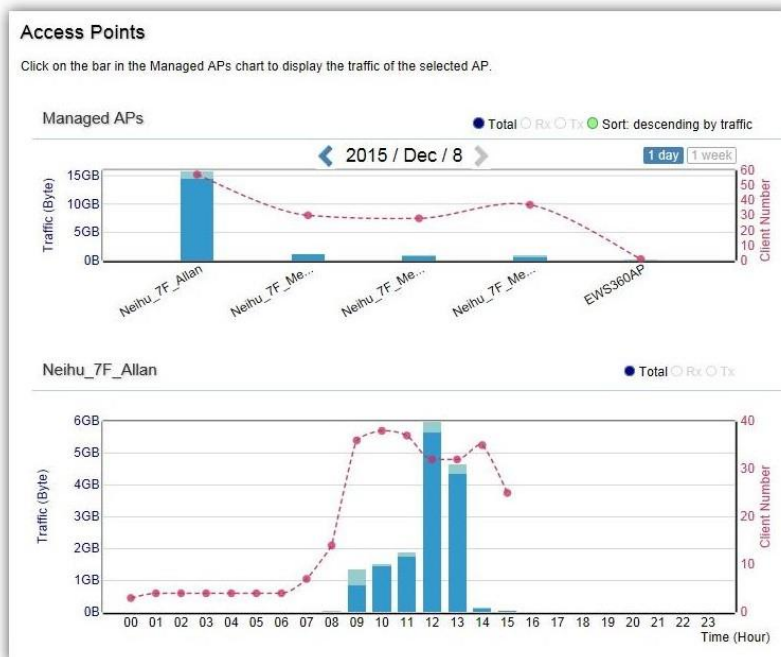
Left click on the Access Point marker to bring up a menu where you can configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

Click on  for the settings to take effect.

Statistics

Access Points

The page displays a visual chart of the network traffic of all the Access Points managed by the ALL-WAPC0450C.



Navigating Tips

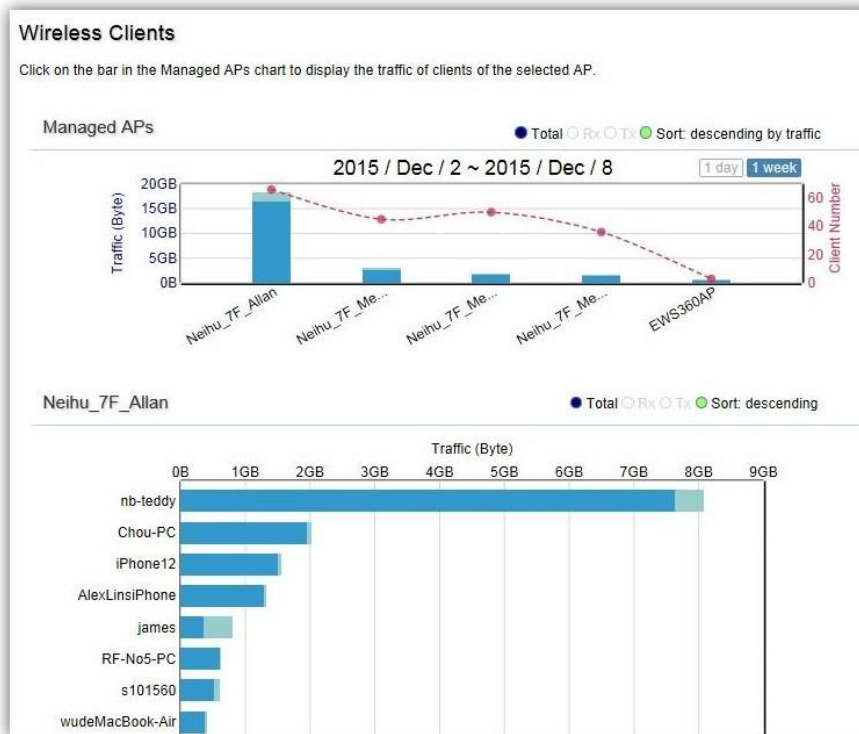
Click **Sort** to sort the order from ascending/descending, depending on your preference.

Click **Rx** to display Rx transmission, **Tx** to display Tx transmission or **Total** to display combined Rx and Tx transmission.

Click **1 day** or **1 week** button to select a time increment to monitor statistics by. Place the mouse cursor over the bar on the chart to show detailed information. Click on the bar in the Managed APs chart to display the traffic of the selected AP.

Wireless Clients

In addition to viewing information based on specific Access Points, you can view data via specific clients as well for security purposes.



Navigating Tips

Click **Sort** to sort the order from ascending/descending, depending on your preference.

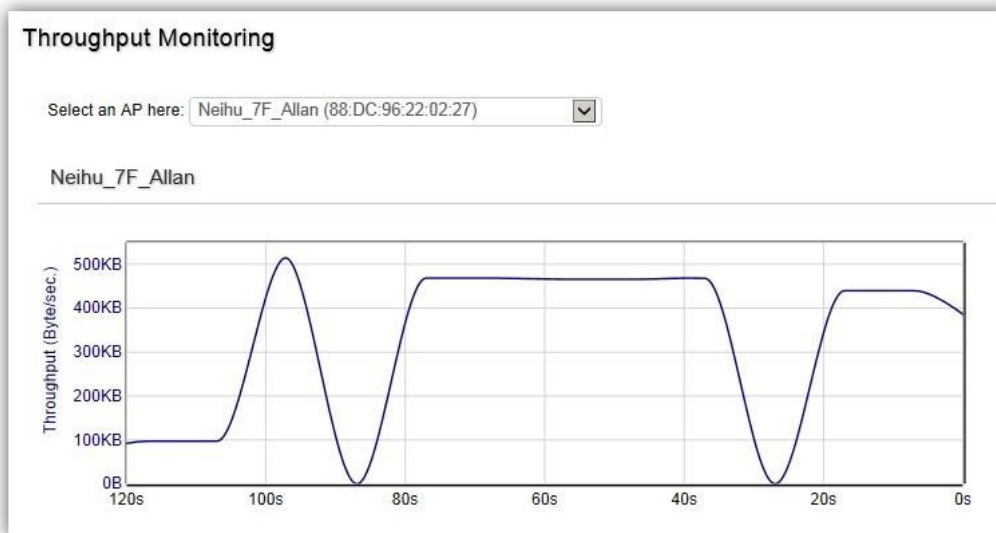
Click **Rx** to display Rx transmission, **Tx** to display Tx transmission or **Total** to display combined Rx and Tx transmission.

Click **1 day** or **1 week** button to select a time increment to monitor statistics by. Place the mouse cursor over the bar on the chart to show detailed information.

Click on the bar in the Managed APs chart to display the wireless clients that has associated with the selected AP.

Real Time Throughput

This page displays the real-time network activity of the selected Access Point.



Hotspot Services

A hotspot is a wireless network that provides access through a captive portal. Use this feature to setup captive portal related configurations.

A captive portal provides registered users with network access while containing unregistered users. Users will need to enter a valid user name and password before they are allowed access to the Internet through the hotspot. Once a Captive Portal Profile is created, the administrator can apply this profile to multiple Guest Networks SSIDs.

Note: Captive portal profiles can only be assigned to the **Guest Network SSIDs**.

Captive Portal

The screenshot displays the 'Captive Portal' configuration interface for an ALLNET device. The left sidebar contains navigation links: Device Management, Monitor, Visualization, Statistics, Hotspot Service (selected), Captive Portal, Guest Account, Mesh, and Maintenance. The main content area is titled 'Captive Portal' and includes a search bar. The configuration is divided into several sections: 'Login Type' with options for 'Splash & go (no authentication)', 'Local User DB', and 'External RADIUS Server'; 'Login Page' with a preview of the splash screen, a 'Logo image' field, a 'Message' field, and a checkbox for 'Enable Term of Use'; 'Redirect Behavior' with options for 'Redirect to the URL that the user was trying to visit' and 'Redirect to a different URL'; and 'User Session' with checkboxes for 'Enable Session Timeout' and 'Enable Idle Timeout', both set to 30 minutes.

Login Type: Defines the mechanism by which a wireless client gains access to the network after the client has associated to the SSID.

Splash & Go	The wireless client is granted network access without any further authentication as soon as it is associates to the SSID.
Local User DB	The wireless client is authenticated using the ALL-WAPC0450C's local database (from <i>Hotspot Service > Guest Account</i>).
External RADIUS Server	The wireless client is authenticated using an external RADIUS server.

Login Page: A splash page is the web page which prompts the user to log in with a user name and password, or accept a network use policy once the client has associated to the SSID.

Local Web Page	Use the splash page hosted locally by ALL-WAPC0450C. The local splash page enable administrators to eliminate the need to set up a local web server. Basic customizations like displaying a corporate logo, custom message and term of use is available.
Redirect users to external URL	External splash page enables the administrator to host their own the splash page web server, rather than having it hosted by the ALL-WAPC0450C.

Redirect Behavior: Configure where users will be redirected after successful login. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected.


Redirect to the URL that the user was trying to visit	Select this option for ezMaster to cache the initial website from the client during the authentication process and then forward it to the originally targeted web server after the user successfully authenticates.
Redirect users to a specified URL after login	Select this option to redirect users to a specific URL after users successfully authenticates.

User Session: Configure session timeout and ideal timeout period.

Session Timeout	Specify a time limit after which users will be disconnected and required to log in again.
Idle Timeout	Specify a time limit for an idle client after which users will be disconnected and required to log in again.

Walled Garden: This option allows users to define network destinations that users can access before authentication. For example, your company's website.

Guest Account



ALL-WAPC0450C4-Port Gigabit L2 Wireless Management Switch

Controller | Switch

Device Management

Monitor

Visualization

Statistics

Hotspot Service

Captive Portal

Guest Account

Mesh

Maintenance

Guest Account

User Name	Password	Description	<div>+ Add</div>
-----------	----------	-------------	------------------

On this page, an administrator can create, edit, and remove user accounts used for captive portal's local database authentication.

Add: Create a new user account.

Remove: Delete the selected user account.

Edit: Edit the settings of the selected user account.

Mesh

The screenshot shows the ALLNET web interface for a 4-Port Gigabit L2 Wireless Management Switch (ALL-WAPC0450C). The top navigation bar includes links for Backup, Upgrade, Reset, Reboot, and Logout. The left sidebar contains a menu with options: Device Management, Monitor, Visualization, Statistics, Hotspot Service, Mesh (selected), Mesh Profile, Node List, Mesh Tools, Isolated Node, and Maintenance. The main content area displays a 'Summary' table with the following information:

Parameter	Value
Controller Version:	1.8.60
Max. Managed APs:	50
IP Address:	192.168.1.239
Base MAC Address:	88:DC:96:02:6F:02
Serial Number:	012345679
System Uptime:	1 hours, 38 mins

1. MESH Profile

Each device must have the same settings in this setting page.

Note: If you have changed the settings in Network Wireless page, please make sure all the settings must be the same in each device.

Mesh AP

Mesh Settings

Mesh Band	<input checked="" type="radio"/> 2.4GHz <input type="radio"/> 5GHz
Mesh ID	<input type="text" value="12345678"/>
Password	<input type="text" value="1234567890"/>
RSSI Threshold	<input type="text" value="-80"/>

Apply

Mesh Band: Select the 2.4GHz or 5GHz for the mesh backbone connection.

Mesh ID: The mesh ID should be maximum up to 8 characters in numbers 0 ~ 9.

Password: The mesh password should be maximum up to 12 characters.

Mesh RSSI: Enter the Mesh RSSI in order to determine the connection procedure which the current wireless link will terminate.

The higher the RSSI number, the stronger the signal.

2. Node List

This Node List page provides easy ways to check the current status of the mesh network. This section contains the following

options:

Mesh Node List

0	0	0
Mesh	Root	offline

Device Name	MAC	Type	Hops Count	Neighbor Nodes
No data available in table				

10 Showing 0 to 0 of 0 entries

◀ Previous Next ▶

All the connected Mesh nodes will be displayed in this page.

Device Name: It shows the device name.

MAC: It shows the device's MAC address.

Type: There are two types of the node. The Root node uplink to the gateway by wire, and connect with other mesh node by wireless simultaneously.

Hops Count: The hops count refers to the number of intermediate devices through which data must pass between the Mesh node itself and Root node. If the Hops Count number is more than 3, we recommend that you have to optimize your deployment of the device location. System shows "—" when the node is Root or alone node

Neighbor Nodes: Display all the neighbor nodes which discovered by individually mesh node, no matter with its signal strength allowed to link or not.

3. Mesh Diag Tools

a. Ping

This page allows you to analyze the connection quality of a mesh node to other mesh node in the mesh network.

Mesh Diag Tools

Mesh Diag Tools

Ping

From To

Number of Pings(1-20):

5

Time out(5-300):

15

Result:

Apply

b. Trace Route

This page allows you to analyze the routing table to a target from a mesh node to other mesh node in the mesh network.

c. Throughput

This page allows you to analyze the throughput from a mesh node to other mesh node in the mesh network.

4. Isolated Nodes

Isolated Nodes feature provides L2 isolation between ports within the same broadcast domain.

Isolated Nodes

Device Name	MAC	Detector Nodes
No data available in table		

10

Showing 0 to 0 of 0 entries

PreviousNext

Maintenance

Schedule Tasks

Schedule Settings

Task Settings

Task Name: (1~32 characters)

Enabled: ☒

Action Settings

Type: ☐ Reboot AP(s) ☐ Change WLAN State ☒ Change Switch PoE State ☐ Switch PoE Reset

Switch Port: 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐

State:

Time Settings

Type: ☒ Day of Week ☐ Date

Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒

Hour Minute

Use the Schedule Tasks feature to control the time(s), or day(s) of a week, or date of a month to automatically perform the following task:

Reboot AP(s): Soft reboot AP

Change WLAN State: Enable/disable WLAN service

NOTE: This feature will not work properly if the ALL-WAPC0450C does not have the correct time settings.

Bulk Upgrade

The Bulk Upgrade feature allows administrators to upgrade the firmware of multiple Access Points at the same time. After uploading the firmware of an AP, the system will automatically display a list of Access Points the system is currently managing that the uploaded firmware is for.

The screenshot shows the ALLNET web interface for a 4-Port Gigabit L2 Wireless Management Switch (ALL-WAPC0450C). The 'Bulk Upgrade' section is active, showing the following information:

Current firmware image information:

Model	Firmware Version	File Name	Image Size(Byte)	Upload Time
ALLWAPC0465AC	v3.0.0-c1.8.60	allwapc0465ac-all-v3.0.0.4_c1.8.60 bin	10974445	2017-Oct-11 09:14:59

Upload Wireless AP firmware image file to controller: [Upload New File](#)
(* Unable to upload new file when APs are under upgrading.)

Device List

[Add to Upgrade](#)

Status	Model	Name	MAC Address	IP Address	Firmware Version
Online	ALL-WAPC0465AC	ALL-WAPC0465AC	88:DC:96:30:97:73	192.168.2.115	v3.0.0-c1.8.60

10 1 to 1 of 1 AP(s) Previous Next

Summary: 1 AVAILABLE, 0 UPGRADING

To upgrade, please follow the steps below:

1. Click on Upload New File to mount AP firmware onto ALL-WAPC0450C flash
2. Once the Access Point firmware is uploaded onto the Controller, the list of Access Points that the uploaded firmware is for will appear in the Device List.
3. Select the Access Points you wish to upgrade and click Add to Upgrade to start the firmware upgrading process.

NOTE: Upgrading APs will temporarily disconnect them (and any associated clients) from the network. To minimize network disruption, we recommend performing the firmware upgrading procedure at an off-peak time.

SSL Certificate

SSL certificates enables device or user identification, as well as secure communications. Administrators can create a self-signed SSL Certificate to secure communications between the Switch and Access Points. Note that Access Points will disconnect and reconnect using new certificate upon applying changes.

SSL Certificate

Create a self-signed SSL Certificate for secured data encryption between Switch and Wireless Access Point(s). AP(s) will reconnect using new certification information upon applying changes.

Generate new certificate

Common Name*:

(1~32 characters)

Organization*:

(1~32 characters)

Organization Unit:

(1~32 characters)

Locality/ City*:

(1~32 characters)

State/ Province*:

(1~32 characters)

Country*:

Afghanistan

Valid Until:

2016/01/07

(2016/1/7 ~ 2037/12/31)

Apply

Certificate Information

Common Name:	Default_name
Organization:	Default_org
Organization Unit:	Default_unit
Locality/ City:	Default_loc
State/ Province:	Default_state
Country:	Taiwan
Valid Date:	1999/12/31 to 2038/01/02

Advanced Option

Restore to Default Certificate:

Restore

Generate New Certificate

Enter the information below to generate a request for an SSL certificate for the controller.

Common Name	Enter the name of the request.
Organization	Enter the organizations name.
Organization Unit	Enter a unit name (department, etc.).
Locality/City	Enter the locality or city.

State/Province	Enter the state or province.
Country	Enter the name of the country.
Valid Date	Enter the expiry date of the certificate.

Restore to Default Certificate

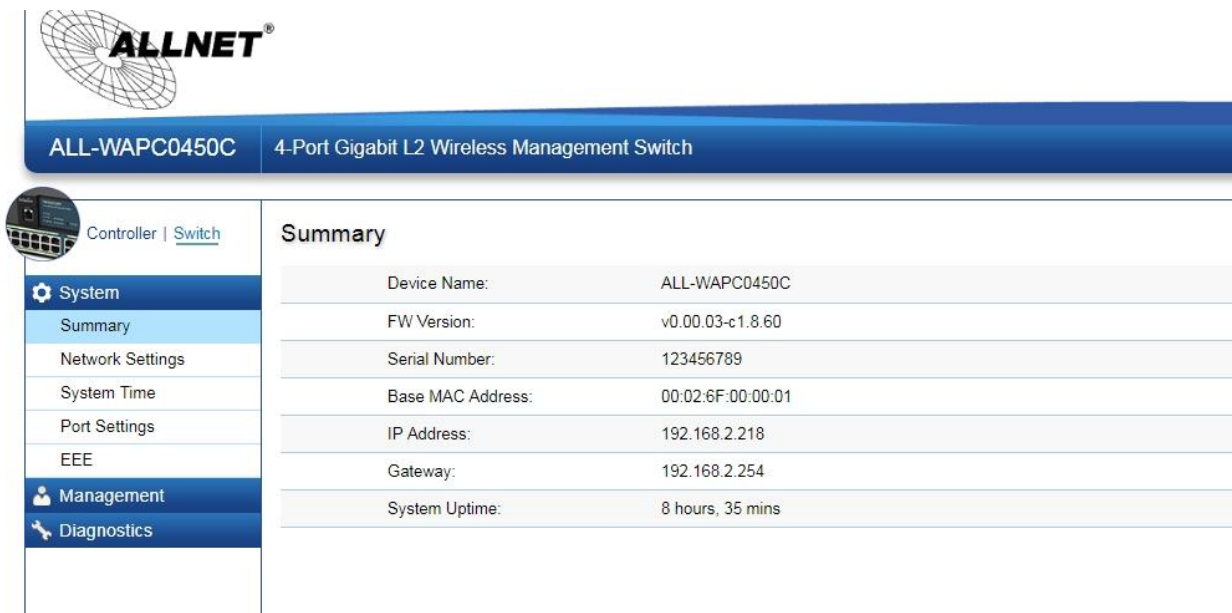
Click on Restore button under Advance Options to restore the default SSL Certificate settings.

Ethernet Switch Features

System

Summary

The Summary page shows general system information for the Switch including the device name, the software version, serial number, MAC address, IP Address, gateway address, and system uptime.



The screenshot displays the ALLNET web interface. At the top, the ALLNET logo is shown next to the device model ALL-WAPC0450C and its description, 4-Port Gigabit L2 Wireless Management Switch. Below this, a navigation menu on the left includes System, Summary, Network Settings, System Time, Port Settings, EEE, Management, and Diagnostics. The main content area is titled 'Summary' and contains a table with the following information:

Device Name:	ALL-WAPC0450C
FW Version:	v0.00.03-c1.8.60
Serial Number:	123456789
Base MAC Address:	00:02:6F:00:00:01
IP Address:	192.168.2.218
Gateway:	192.168.2.254
System Uptime:	8 hours, 35 mins

Device Name	Displays the model name of the device.
FW Version	Displays the installed firmware version of the device.
Serial Number	Displays the serial number of the device.
Base MAC Address	Displays the MAC address of the device.
IP Address	Displays the IP address of the device.
Gateway	Displays the Gateway IP address.
System Uptime	Displays the number of days, hours, and minutes since the last system restart. The System Uptime is displayed in the following format: days, hours, and minutes.

Network Settings

The Network Setting screen contains fields for assigning IP addresses. IP addresses are either defined as static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

To access the page, click **IP Settings** under the **System** menu.

IPv4

Select whether to you wish to enable Static or DHCP for auto-configuration. Next, enter the information for the IP address, gateway, and DNS servers.

IPv4

IPv4 Address Settings

Auto Configuration: ☒ Static ☐ DHCP

IPv4 Address: 10.0.85.245

Subnet Mask: 255.255.255.0

Gateway: 10.0.85.254

DNS Server 1: 10.0.91.240

DNS Server 2: 0.0.0.0

Apply



Important:

If the device fails to retrieve an IP address through DHCP, the default IP address is **192.168.0.239** and the factory default subnet mask is **255.255.255.0**.

Dynamic IP Address (DHCP)	Enables the IP address to be configured automatically by the DHCP server. Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, default gateway IP address, and a domain name server IP address automatically. Selecting this field disables the IP Address, Subnet Mask, and Gateway fields.
Static IP Address	Allows the entry of an IP address, subnet mask, and a default gateway for

	the Switch. Select this option if you don't have a DHCP server or if you wish to assign a static IP address to the Switch.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface. Enter the IP address of your Switch in dotted decimal notation. The factory default value is: 192.168.0.239
Subnet Mask	A subnet mask separates the IP address into the network and host addresses. A bitmask that determines the extent of the subnet that the Switch is on. This should be labeled in the form: xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimals) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. Enter the IP subnet mask of your Switch in dotted decimal notation. The factory default value is: 255.255.255.0
Gateway	Enter an IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway your network is not part of an Intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field blank.
DNS Server (Domain Name System)	Used for mapping a domain name to its corresponding IP addresses and vice versa. Enter a DNS IP address in order to be able to use a domain name to access the Switch instead of using an IP address.

Click **Apply** to save settings.

IPv6

IPv6 is an upgraded version to IPv4, providing more available IP addresses as well as other benefits. To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway). To configure IPv6 for the Switch, select whether to you wish to enable **Auto-Configuration**, **Static**, or **DHCPv6 Client**. Next, enter the information for the IP address, range, and gateway.

IPv6

IPv6 Address Settings

IPv6 State: Auto Configuration

IPv6 Address:

/

0

(1-127)

Gateway:

Link Local Address: fe80::213:64ff:fe00:1500

Apply

IPv6 State	Select whether you wish to enable Auto Configuration, DHCPv6 Client, or Static for the IPv6 address.
Auto Configuration	Use this option to set the IPv6 address for the IPv6 network interface in Auto Configuration. The Switch will automatically generate and use a globally-unique IPv6 address based on the network prefix and its Ethernet MAC address.
DHCPv6 Client	This enables the IP address to be configured automatically by the DHCP server. Select this option if you have an IPv6 DHCP server that can assign the Switch an IPv6 address/prefix and a default gateway IP address.
Static	Allows the entry of an IPv6 address/prefix and a default gateway for the Switch. Select this option if you wish to assign static IPv6 address information to the Switch.
IPv6 Address	This field allows the entry of an IPv6 address/prefix to be assigned to this IP interface.
Gateway	Set the default gateway IPv6 address for the interface. Enter the default gateway IPv6 address.

Click **Apply** to save settings.

System Time

Use the System Time screen to view and adjust date and time settings.

The Switch supports Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. This switch operates only as an SNTP client and cannot provide time services to other systems.

System Time

Settings

Current Time: 2015/Dec/09 15:48:41

Enable SNTP: ☒ Enabled ☐ Disabled

Time Zone: Set by time (GMT +8 : 0)

Daylight Savings Time: Disabled

SNTP/NTP Server Address: time.stdtime.gov.tw (x.x.x.x or Hostname)

Server Port: 123 (1 - 65535 | Default : 123)

Apply

Current time	Displays the current system time.
Enable SNTP	Select whether to enable or disable system time synchronization with an SNTP server.
Time Zone	Configure the time zone setting either by setting GMT difference or by country.
Daylight Savings Time	Select from Disabled, Recurring or Non-recurring.
Daylight Savings Time Offset	Enter the time of Daylight Savings Time Offset.
Recurring From	Select the Day, Week, Month, and Hour from the list.
Recurring To	Select the Day, Week, Month, and Hour from the list.
SNTP/NTP Server Address	Enter the IP address or hostname of the SNTP/NTP server.
Server Port	Enter the server port of the SNTP/NTP server.

To configure date/time through SNMP:

1. Next to the Enable SNMP, select Enable.
2. In the Time Zone Offset list, select by country or by the GMT time zone in which the Switch is located.
3. Next select Disabled, Recurring, or Non-Recurring for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
4. In the SNTP/NTP Server Address field, enter the IP address or the host name of the SNTP/NTP server.
5. Finally, enter the port number on the SNTP server to which SNTP requests are sent. The valid range is from 1–65535. The default is: 123.
6. Click Apply to update the system settings.

To configure date/time manually:

1. Next to the Enable SNMP, select Disable.
2. In the Manual Time field, use the drop-down boxes to manually select the date and time you wish to set.
3. In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.
4. Next select Disabled, Recurring or Non-recurring for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
5. Click Apply to update the system settings.

Port Settings

Use this screen to view and configure Switch port settings. The Port Settings page allows you change the configuration of the ports on the Switch in order to find the best balance of speed and flow control according to your preferences. Configuring Gigabit ports require additional factors to be considered when arranging your preferences for the Switch compared to 10/100 ports.

To access the page, click **Port Settings** under the **System** menu.

Port Settings				
	Port	Link Status	Mode	Flow Control
<input type="checkbox"/>			Auto <input type="button" value="v"/>	Disabled <input type="button" value="v"/>
<input type="checkbox"/>	1	Link Down	Auto	Disabled
<input type="checkbox"/>	2	Link Down	Auto	Disabled
<input type="checkbox"/>	3	Link Down	Auto	Disabled
<input type="checkbox"/>	4	Link Down	Auto	Disabled
<input type="checkbox"/>	5	Link Down	Auto	Disabled
<input type="checkbox"/>	6	Link Down	Auto	Disabled
<input type="checkbox"/>	7	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	8	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	9	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	10	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	11	Link Down	Auto	Disabled
<input type="checkbox"/>	12	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk1	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk2	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk3	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk4	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk5	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk6	Link Down	Auto	Disabled

Port	Displays the port number.
Link Status	Indicates whether the link is up or down.
Mode	<p>Select the speed and the duplex mode of the Ethernet connection on this port.</p> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port</p>

	uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.</p>

Click **Apply** to save settings.

EEE

Energy Efficient Ethernet (EEE), an Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard, reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits shut down when there is no traffic.

Network administrators have long focused on the energy efficiency of their infrastructure, and the EnGenius Layer 2 Switch complies with the IEEE's Energy-Efficient Ethernet (EEE) standard. The EEE compliant Switch offers users the ability to utilize power that Ethernet links use only during data transmission. Lower Power Idle (LPI) is the method for achieving the power saving during Ethernet ideal time.

Use the **EEE** configuration page to configure Energy Efficient Ethernet.

Energy-Efficient Ethernet		
<input type="checkbox"/>	Port	EEE Status
<input type="checkbox"/>		Disabled <input type="button" value="v"/>
<input type="checkbox"/>	1	Disabled
<input type="checkbox"/>	2	Disabled
<input type="checkbox"/>	3	Disabled
<input type="checkbox"/>	4	Disabled
<input type="checkbox"/>	5	Disabled
<input type="checkbox"/>	6	Disabled
<input type="checkbox"/>	7	Disabled
<input type="checkbox"/>	8	Disabled
<input type="checkbox"/>	9	Disabled
<input type="checkbox"/>	10	Disabled

Port	Display the port for which the EEE setting is displayed.
EEE Status	Enable or disable EEE for the specified port.

Click **Apply** to save settings.

Management

System Information

The System Information screen contains general device information including the system name, system location, and system contact for the Switch.

System Information

Information

System Name: Nelhu-7F-EWS5912FP (char : 1 ~ 255)

System Location: Default Location (char : 0 ~ 255)

System Contact: Default Contact (char : 0 ~ 255)

Apply

System Name	Enter the name you wish to use to identify the Switch. You can use up to 255 alphanumeric characters.
System Location	Enter the location of the Switch. You can use up to 255 alphanumeric characters. The factory default is: Default Location.
System Contact	Enter the contact person for the Switch. You can use up to 255 alphanumeric characters. The factory default is: Default Location.

Click **Apply** to update the system settings.

User Management

Use the User Management page to control management access to the Switch based on manually configured user names and passwords. A User account can only view settings without the right to configure the Switch, and an Admin account can configure all the functions of the Switch. Click the Add button to add an account or the Edit button to edit an existing account.

User Name	Password Type	Password	Password Retype	Privilege Type	
admin	Encrypted			Admin	

User Name	Enter a username. You can use up to 18 alphanumeric characters.
Password Type	Select Clear Text or Encrypted from the list.
Password	Enter a new password for accessing the Switch.
Password Retype	Repeat the new password used to access the Switch.
Privilege Type	Select Admin or User from the list to regulate access rights.



Important:

Note that Admin users have full access rights to the Switch when determining the authority of the user account.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Dual Image

The Switch maintains two versions of the Switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image.

Dual Image

Active	Flash Partition	Status	Image Name	Image Size(Byte)	Created Time
<input type="radio"/>	Partition 0	Backup	IMG-1.05.16-c1.5.3	8273849	2015-07-07 21:50:12
<input checked="" type="radio"/>	Partition 1	Active	IMG-1.05.26-c1.6.24	7320132	2015-11-13 13:38:03

Apply

Active	Selects the partition you wish to be active.
Flash Partition	Displays the number of the partition.
Status	Displays the partition which is currently active on the Switch.
Image Name	Displays the name/version number of the image
Image Size	Displays the size of the image file.
Created Time	Displays the time the image was created.

Click **Apply** to update the system settings.

Diagnostics

Cable Diagnostics

Cable Diagnostics helps you to detect whether your cable has connectivity problems provides information about where errors have occurred in the cable. The tests use Time Domain Reflectometry (TDR) technology to test the quality of a copper cable attached to a port. TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. All or part of the signal is reflected back either by cable defects or by the end of the cable when an issue is present. Cables are tested when the ports are in the down state, with the exception of the cable length test.

Cable Diagnostics
Note: Cable length is only for reference and may be inaccurate when 'OK' is indicated.

Port	Pair A	Cable Length A (meter)	Pair B	Cable Length B (meter)	Pair C	Cable Length C (meter)	Pair D	Cable Length D (meter)
Port 2 <input type="checkbox"/>	OK	8	OK	8	OK	8	OK	8

Test

To verify accuracy of the test, it is recommended that you run multiple tests in case of test fault or user error.

Click **Test** to perform the cable tests for the selected port.

Ping Test

The Packet Internet Groper (Ping)Test allows you to verify connectivity to remote hosts. The Ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss. Send a ping request to a specified IPv4 address. Check whether the Switch can communicate with a particular network host before testing.

Ping Test

Ping Test Settings

IP Address: (x.x.x.x or hostname)

Count: (1 - 5 | Default : 4)

Interval (in sec): (1 - 5 | Default : 1)

Size (in bytes): (8 - 5120 | Default : 56)

Result:

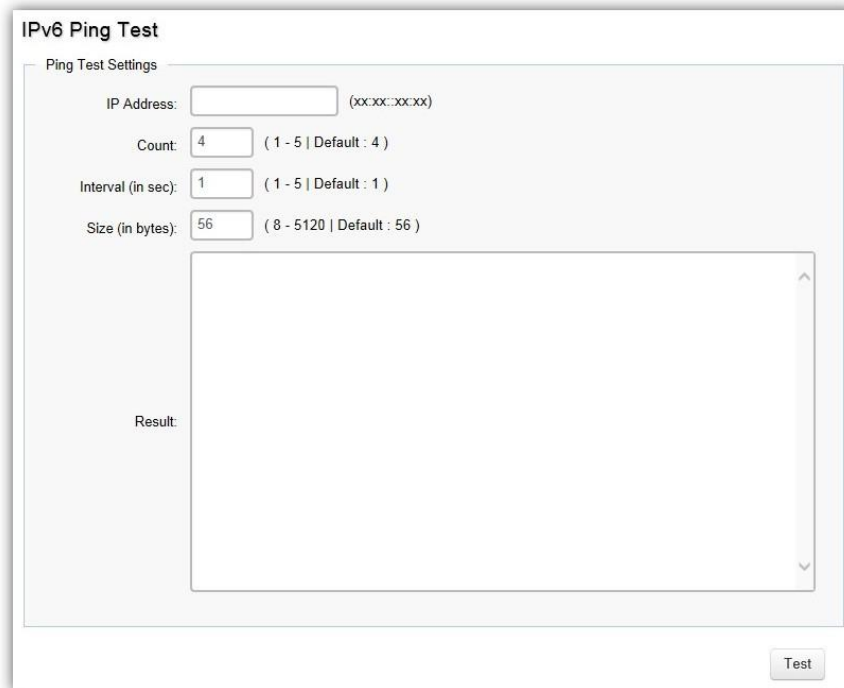
You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

IP Address	Enter the IP address or the host name of the station you want the Switch to ping to.
Count	Enter the number of ping to send. The range is from 1 to 5 and the default is 4.
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

Click **Test** to perform the ping test.

IPv6 Ping Test

Send a ping request to a specified IPv6 address. Check whether the Switch can communicate with a particular network host before testing.



The image shows a web-based configuration window titled "IPv6 Ping Test". It contains a "Ping Test Settings" section with four input fields: "IP Address" (with a placeholder "xxxx:xxxx"), "Count" (set to 4, range 1-5, default 4), "Interval (in sec)" (set to 1, range 1-5, default 1), and "Size (in bytes)" (set to 56, range 8-5120, default 56). Below these is a large "Result" text area. A "Test" button is located at the bottom right of the window.

You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

IP Address	Enter the IPv6 address or the host name of the station you want the Switch to ping to.
Count	Enter the number of ping to send. The range is from 1 to 5 and the default is 4.
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

Click **Test** to perform the ping test.

Trace Route

The traceroute feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination, or fails to reach the destination and is discarded. In testing, it will tell you how long each hop from router to router takes via the trip time of the packets it sends and receives from each successive host in the route.

Trace Route

Trace Route Settings

IP Address:

google.com

(x.x.x.x or hostname)

Max Hop:

30

(2 - 255 | Default : 30)

Result:

traceroute to google.com (64.233.187.101), 30 hops max, 40 byte packets

1 118.163.20.254 (118.163.20.254) 48 bytes to 10.0.85.245 20 ms 20 ms 10 ms

2 168.95.228.42 (168.95.228.42) 36 bytes to 10.0.85.245 20 ms 30 ms 20 ms

3 220.128.2.158 (220.128.2.158) 148 bytes to 10.0.85.245 20 ms 220.128.3.102 (220.128.3.102) 148 bytes to 10.0.85.245 20 ms 220.128.1.70 (220.128.1.70) 148 bytes to 10.0.85.245 20 ms

4 220.128.9.81 (220.128.9.81) 148 bytes to 10.0.85.245 20 ms 20 ms 220.128.8.81 (220.128.8.81) 148 bytes to 10.0.85.245 20 ms

5 220.128.9.173 (220.128.9.173) 36 bytes to 10.0.85.245 20 ms 220.128.8.173 (220.128.8.173) 36 bytes to 10.0.85.245 20 ms 220.128.9.173 (220.128.9.173) 36 bytes to 10.0.85.245 20 ms

6 72.14.196.3 (72.14.196.3) 36 bytes to 10.0.85.245 20 ms 74.125.49.158 (74.125.49.158) 36 bytes to 10.0.85.245 20 ms 20 ms

7 209.85.243.30 (209.85.243.30) 36 bytes to 10.0.85.245 30 ms 30 ms 20 ms

8 216.239.46.223 (216.239.46.223) 148 bytes to 10.0.85.245 30 ms 209.85.250.229 (209.85.250.229) 148 bytes to 10.0.85.245 20 ms 209.85.252.213 (209.85.252.213) 148 bytes to 10.0.85.245 30 ms

9 216.239.43.101 (216.239.43.101) 36 bytes to 10.0.85.245 20 ms 66.249.94.131 (66.249.94.131) 36 bytes to 10.0.85.245 20 ms 216.239.50.45 (216.239.50.45) 36 bytes to 10.0.85.245 30 ms

Test

IP Address	Enter the IP address or the host name of the station you wish the Switch to ping to.
Max Hop	Enter the maximum number of hops. The range is from 2 to 255 and the default is 30.
Result	Displays the trace route results.

Click **Test** to initiate the trace route

For more information and help, see the Service Portal at <http://service.allnet.de>

Hiermit erklärt ALLNET GmbH Computersysteme, dass sich das Gerät **ALL-WAPC0450C** in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EC oder 2014/53/EU befindet. Die Konformitätserklärung kann unter folgender Adresse gefunden werden: www.allnet.de/downloads.html

ALLNET GmbH Computersysteme declares that the device **ALL-WAPC0450C** is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC or 2014/53/EU. The Declaration of conformity can be found under this link: www.allnet.de/downloads.html

EU contact:

ALLNET GmbH Computersysteme
Maistrasse 2
82110 Germering

Tel. +49 (0)89 894 222 - 22
Fax +49 (0)89 894 222 - 33
Email: [info\(at\)allnet.de](mailto:info(at)allnet.de)



CE Marking is the symbol as shown on the top of this page. The letters "CE" are the abbreviation of French phrase "Conformity European" which literally means "European Conformity". The term initially used was "EC Mark" and it was officially replaced by "CE Marking" in the Directive 93/68/EEC in 1993. "CE Marking" is now used in all EU official documents.



This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

This recycle logo Indicates that this product is capable of being recycled, not that the product has been recycled or will be accepted in all recycling collection systems.



This symbol is **new RED** aligns the previous directive with the New Legislative Framework for the marketing of products. The revision takes account of the need for improved market surveillance, in particular for the traceability obligations of manufacturers, importers and distributors. It provides improved instruments for market surveillance, such as the possibility to require prior registration of radio equipment, within those categories affected by low levels of compliance. The Directive requires **equipment to be constructed for efficient use of the radio spectrum, as well as electromagnetic compatibility, to avoid interference with terrestrial and orbital communications.**



The RoHS directive aims to restrict certain dangerous substances commonly used in electronic and electronic equipment. This [RoHS compliant](#) symbol indicate the component is [tested](#) for the presence of Lead (Pb), Cadmium (Cd), Mercury (Hg), Hexavalent chromium (Hex-Cr), Polybrominated biphenyls (PBB), and Polybrominated diphenyl ethers (PBDE). For Cadmium and Hexavalent chromium, there must be less than 0.01% of the substance by weight at raw homogeneous materials level. For Lead, PBB, and PBDE, there must be no more than 0.1% of the material, when calculated by weight at raw homogeneous materials. Any RoHS compliant component must have 100 ppm or less of mercury and the mercury must not have been intentionally added to the component.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do not open the device. Opening or removing the device cover can expose you to dangerous high voltage points or other risks. Only qualified service personnel can service the device. Please contact your vendor for further information.
- Do not use your device during a thunderstorm. There may be a risk of electric shock brought about by lightning.
- Do not expose your device to dust or corrosive liquids.
- Do not use this product near water sources.
- Make sure to connect the cables to the correct ports.
- Do not obstruct the ventilation slots on the device.

DISCLAIMER_OF_WARRANTY

This Program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This Program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this Program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The full text of the GNU General Public License version 2 is included with the software distribution in the file LICENSE.GPLv2

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Written Offer for Source Code

For binaries that you receive from ALLNET GmbH Computersysteme on physical media or within the download of the offered firmware that are licensed under any version of the GNU General Public License (GPL) or the GNU LGPL, you can receive a complete machine-readable copy of the source code by sending a written request to:

ALLNET GmbH Computersysteme
Maistrasse 2
82110 Germering

Your request should include: (i) the name of the covered binary, (ii) the version number of the ALLNET product containing the covered binary, (iii) your name, (iv) your company name (if applicable) and (v) your return mailing and email address (if available). We may charge you a nominal fee to cover the cost of the media and distribution. Your request must be sent within three (3) years of the date you received the GPL or LGPL covered code. For your convenience, some or all of the source code may also be found at:

<http://www.allnet.de/gpl.html>

LICENSE.GPLv2

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the

files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based

on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding

source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues),

conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free

Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General

Public License instead of this License.

LICENSE.LGPLv2.1

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source

code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to

encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for

making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has

a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which

must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies

the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with

this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library

specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the

ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!