DeskPoint Pro™

User and Installation Manual

TA-6950

TA-7950

TA-8050

teleadapt

Keeping Your World Connected™

Table of Contents

1. Features

The DeskPoint Pro is designed for use in hotel rooms and combines 802.11n, IEEE 802.11g and IEEE 802.11b wireless technology to provide the best wireless performance, enabling client computers to access the resources on the hotel Ethernet network. With the Web-based user interface or SNMP a network administrator can easily and clearly manage the DeskPoint Pro.

Desktop or Under Desk

- **Desktop -** The TA-6960 and TA-7950 are on desk models. The TA-6950 incorporates a retractable spool whereas the TA-7950 has a RJ45 socket.
- **Under Desk -** The TA-8050 is designed to fit unobtrusively under the a desk in the guest room and can be used in conjunction with other TeleAdapt cable management products.

IEEE 802.11n

- **RF type selection -** The RF type of the wireless interface can be configured to work in IEEE 802.11n only , IEEE 802.11b only, IEEE 802.11g only, or mixed mode (802.11n, 802.11g and 802.11b simultaneously).
- **64-bit and 128-bit WEP (Wired Equivalent Privacy) -** For authentication and data encryption.
- **Enabling/Disabling SSID broadcasts -** The administrator can enable or disable the SSID broadcasts functionality for security reasons. The correct SSID has to be specified on client computers.
- **IEEE 802.1x/RADIUS -** The DeskPoint Pro can be configured to authenticate wireless users and distribute encryption keys dynamically by IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service).

- **WPA (Wi-Fi Protected Access) -** The DeskPoint Pro supports the WPA standard proposed by the Wi-Fi Alliance (Hhttp://www.wi-fi.orgH). Both WPA-PSK (Pre-Shared Key) mode and full WPA mode are supported. WPA is composed of TKIP (Temporal Key Integrity Protocol) and IEEE 802.1x and serves as a successor to WEP for better WLAN security.
- **WPA2 (Wi-Fi Protected Access 2) -** This advanced protocol implements the mandatory elements of 802.11i. WPA2 is an improvement on the WPA-PSK standard, and is simply using a shared password for access to your network. Only users with this password can access your network.
- **Client isolation -** Wireless-to-wireless traffic can be blocked so that the wireless clients cannot see each other. This function also blocks wired clients from accessing Wireless clients.
- **Transmit power control -** Transmit power of the DeskPoint Pro's RF module can be adjusted to change RF coverage.
- **Associated wireless clients status -** The DeskPoint Pro can show the status of all wireless clients that are associated with it.
- H**DHCP Client -** The DeskPoint Pro can automatically obtain an IP address from a DHCP server.
- H**Packet Filtering.**H The DeskPoint Pro provides Layer 2, Layer 3, and Layer 4 filtering capabilities.

Firmware Tools

- **Firmware upgrade -** The firmware can be upgraded by HTTP (Hyper Text Transfer Protocol).

- **Configuration backup -** The configuration settings can be backed up to a file via HTTP for later restoring.
- **Configuration reset -** Resetting the configuration settings to factory-default values.

Management

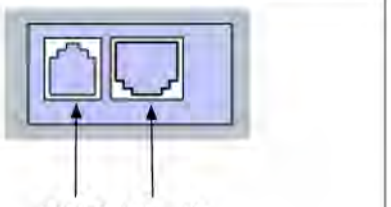
- **Web-based Network Manager** for configuring and monitoring the DeskPoint Pro via a Web browser (Internet Explorer, Firefox or Google Chrome). The management protocol is HTTP (Hyper Text Transfer Protocol)-based.
- **SNMP -** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, and Private Enterprise MIB are supported.
- **System log -** For system operational status monitoring.
  - **Local log -** System events are logged to the on-board RAM of the DeskPoint Pro and can be viewed using a Web browser.
  - **Remote log by SNMP trap -** Systems events are sent in the form of SNMP traps to a remote SNMP management server.

Power Charging

- **USB Charging** 5V for charging mobile devices

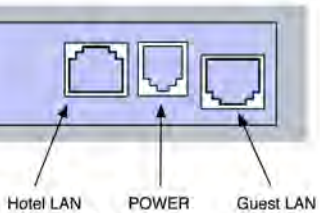
LED Definitions

- **TA-6950 and TA-7950 -** At the front of the device, there are 3 LED indicators. See Figure 1 below for description of each LED indication.
- **TA-8050 -** On top of the device, there are LED indicators. See Figure 2 below for description of each LED indication.



TA-6950-TA-7950

Connector	Description
Power	Power connector with 5V/2A
Hotel LAN	Wired connection to hotel network
Guest LAN	Wired connection for Guest access



TA-8050

Connector	Description
Hotel LAN	Wired connection to hotel network
POWER	Power connector with 5V/2A
Guest LAN	Wired connection for Guest access

The Front LEDs of TA-6950/TA-7950

LED	State	Description
PWR	ON	Power on
RF	ON	RF on and blink every second
	OFF	RF off
LAN	ON	LAN on
	Flashing	Throughput is busy
	OFF	LAN off

The Front LEDs of TA-8050

LED	State	Description
PWR	ON	Power on
RF	ON	RF on and blink every second
LAN	ON	LAN on
	Flashing	Throughput is busy
	OFF	LAN off

Connections

- **The TA-6950 and TA-7950** also provide a wired Guest LAN interface just above the indicator LEDs. For the TA-6950 this is a retractable spool, for the TA-7950 this is an RJ45 socket. Both models also provide a USB socket that can provide up to 5V/1A for charging mobile devices. See Figure 3 to the left.

  TA-8050 provides an RJ45 jack to be used for offering a wired access point for the guest. Pair a TeleAdapt Pull-Through Pro or other Internet AP product for best presentation to the guest. See Figure 4 to the left.

Hardware Reset

The reset button can be found on the bottom of the unit. To perform a factory reset press and hold the reset button until the LAN LED flashes. When the LAN LED flashes release the reset button and quickly press and hold the reset button a second time (for at least 10 seconds) until the LAN LED flashes again.

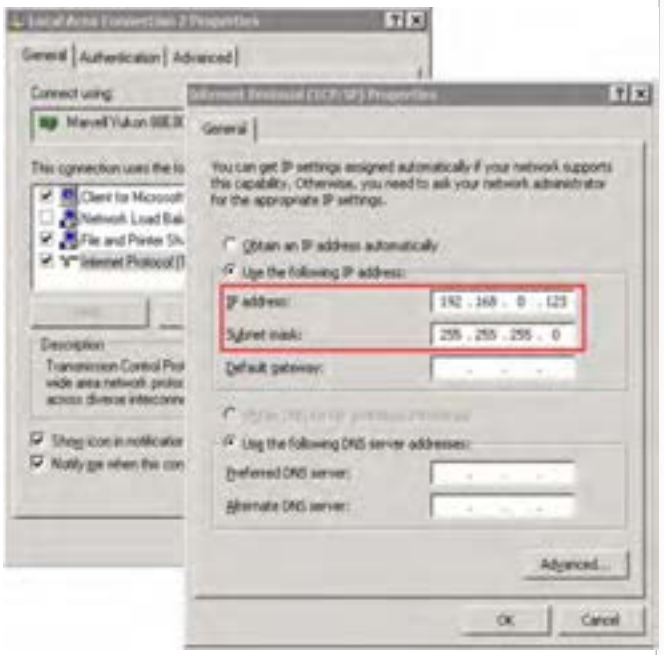


Fig 1. An example of Internet Protocol (TCP/IP) Properties in Microsoft Windows

Note: For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

2. Installing and Configuring DeskPoint Pro

This section offers information about installing your DeskPoint Pro. Before configuring the DeskPoint Pro, you need to know the connection information supplied by your service provider and the field application environment.

Preparing for Configuration

To configure the DeskPoint Pro, a computer with a web browser is needed. For the first-time or maintenance configuration of the DeskPoint Pro, an Ethernet network interface card (NIC) should have been installed in the managing computer.

Since the configuration/management protocol is HTTP-based, you have to make sure that the IP address of the managing computer and the IP address of the managed DeskPoint Pro are in the same IP subnet (the default IP address of the DeskPoint Pro is **192.168.0.1** and the default subnet mask is **255.255.255.0**.)

Connecting the Managing Computer

Using Ethernet Cable to connect the managing computer and the Wireless 11n Access Point as following figure shows. One end of the Ethernet cable must be plugged into the **Hotel** LAN Ethernet jack of the DeskPoint Pro for configuration.

Changing the TCP/IP Settings of the Managing Computer

Use the **Windows Network Control Panel Applet** to change the TCP/IP settings of the managing computer, so that the IP address of the computer and the IP address of the DeskPoint Pro are in the same IP subnet. Set the IP address of the computer to **192.168.0.xxx** (the default IP address of the DeskPoint Pro is **192.168.0.1**) and the subnet mask to **255.255.255.0.**

Default User Name and Password

The default user name is ‘root’ and the default password is ‘root’.

3. Web Configuration

NOTE: All management services on the DeskPoint Pro are restricted so they are only accessible via the Hotel LAN port.

Summary

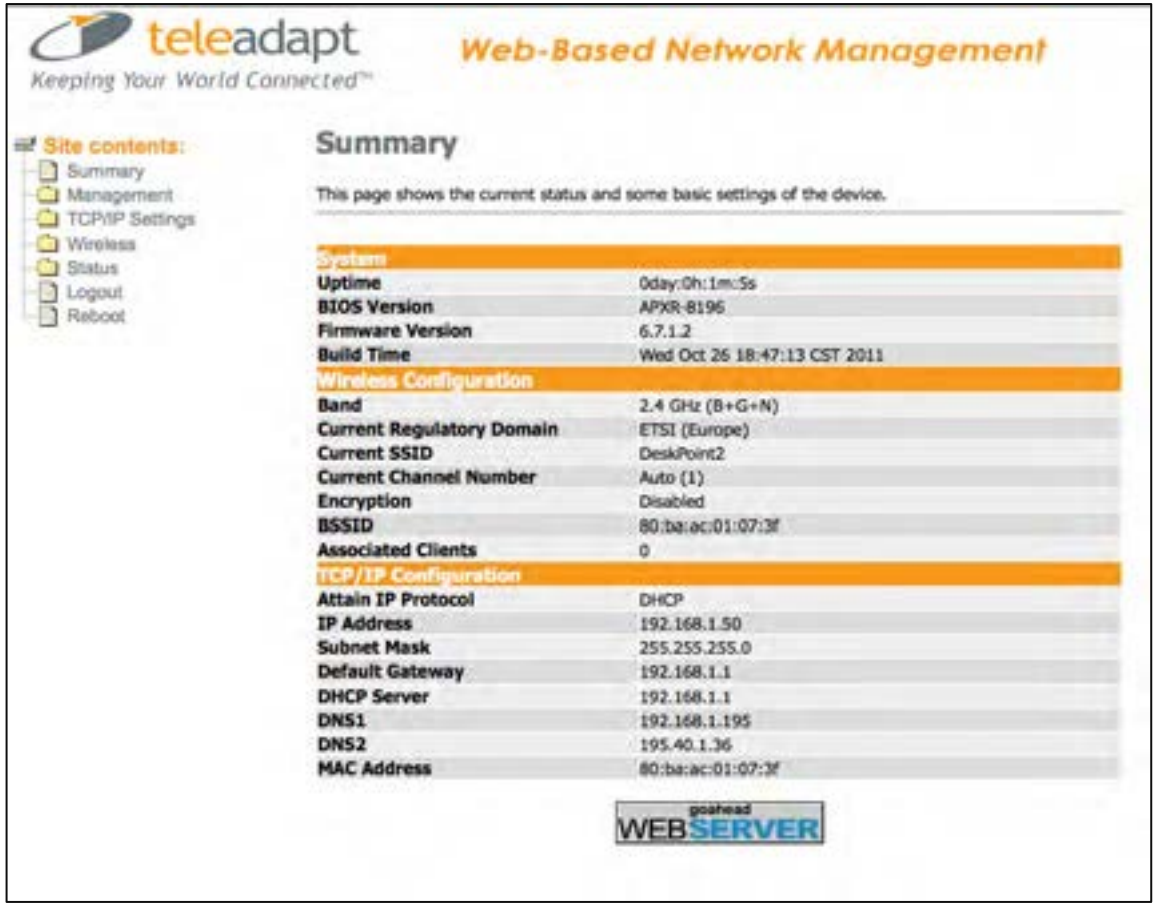


Fig 1. The Summary page

Menu Structure

The left side of the Home page contains a menu for you to carry out commands. Here is a brief description of the hyperlinks on the menu:

Summary. For configuration setting summary.

Management. System monitoring information

- **Firmware Tools -** For upgrading the firmware of the DeskPoint Pro and backing up and restoring configuration settings of the DeskPoint Pro.
- **System Setting -** For changing the account info and web access info for the web server of the DeskPoint Pro.
- **System Tools -** Ping Tool, ARP Tool and trace route tool.
- **Time Zone -** Time zone and SNTP (Simple Network Time Protocol) server settings.
- **SNMP -** Simple Network Management Protocol (SNMP) agent settings and SNMP trap table.

TCP/IP. TCP/IP-related settings.

- **LAN.** IP addressing settings for the DeskPoint Pro.
- **VLAN Tag.** settings.

Wireless. IEEE 802.11n-related settings.

- **Basic Settings -** Basic settings for the IEEE 802.11b/g/n interface of the DeskPoint Pro to work properly with wireless clients.
- **Advanced Settings -** Advanced settings for the more technically users who have a sufficient knowledge about the Wireless LAN.
- **Security -** Security settings for authenticating wireless users and encrypting wireless data. Include the IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service) settings for better wireless security.

- **Access Control -** Wireless Access Control settings.
- **Status -** System monitoring information.
- **Network Status -** Shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.
- **System Log -** System events log.
- **Active Clients -** Display the status of all wireless clients who associated to the DeskPoint Pro.
- **Logout -** The Logoff page.

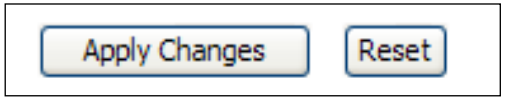


Fig 2. Click Apply Changes to store settings.

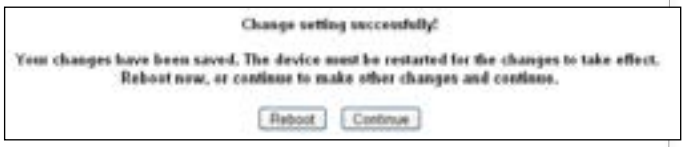


Fig 3. Save, Save & Restart, and Cancel.

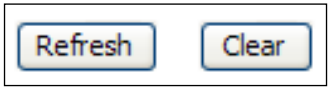


Fig 4. Refresh and Clear

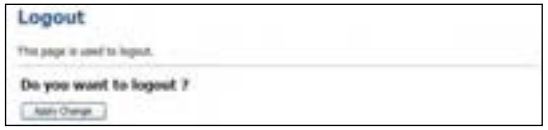


Fig 5. Logoff Page

Apply Changes, Reset, Reboot and Continue Commands

Normally at the bottom of each setting page, there are two buttons - **Apply Changes and Reset**. Clicking **Apply Changes** stores the settings changes to the memory of the DeskPoint Pro and brings you back to the next page to choose the next step. Clicking **Reset** discards any settings changes and brings you back to the start page.

Clicking **Reboot** to restarts the DeskPoint Pro immediately for the settings changes to take effect. Clicking **Continue** moves to other page for change other settings.

Refresh and Clear Commands

At the bottom of each status page that shows read-only information, Clicking **Refresh** updates the shown status information. And in the System log page the **Clear** immediately clean system log.

Logout Commands

The page provide user to log off the Web management immediately. User needs apply account and password again if they want to login again.

Fig 6. Firmware Management via HTTP

Fig 7. Firmware Management via TFTP

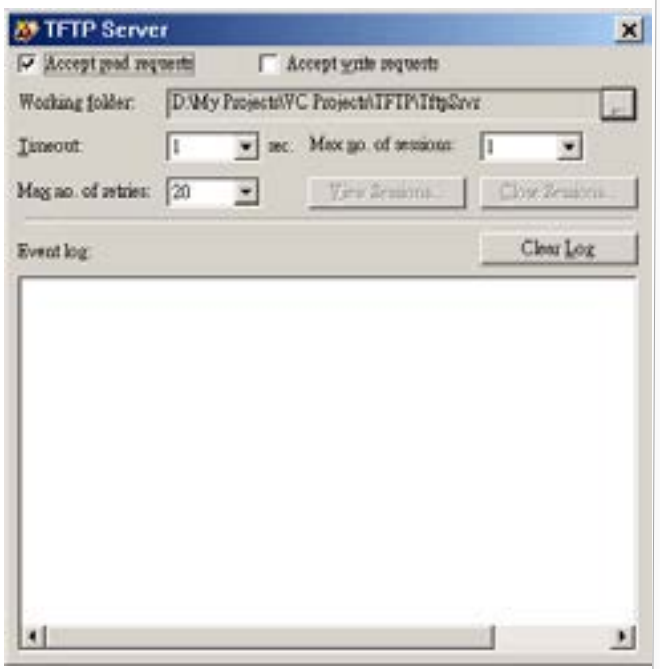


Fig 8. TFTP Server

Firmware Tools

Firmware management operations for the DeskPoint Pro include **firmware upgrade**, configuration backup (**Load Settings**), configuration restore (**Save Settings**), and configuration reset (**Load Factory Default**). Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP. Due to different behavior of different Web browser types and versions, HTTP-based firmware management operations may not work properly with some Web browsers.

When using TFTP as the firmware management protocol, you can configure settings the DeskPoint Pro's TFTP client to communicate with a TFTP server. Ensure that the TFTP Server IP uses the same subnet to prevent errors arising.

Screen capture to the left is the TFTP Server in Windows XP, the TftpSrvr. Please note:

- After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.
- Make sure the Accept read requests check box of TFTP Server is selected.
- The LAN IP address of the DeskPoint Pro and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.
- After the firmware is upgraded, be sure to delete the contents of the Web browser cache, so that the Web management pages can be shown correctly.
- A failed upgrade may corrupt the firmware and make the DeskPoint Pro inaccessible.

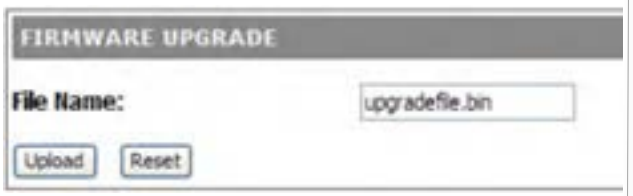


Fig 9. Firmware upgrade by HTTP

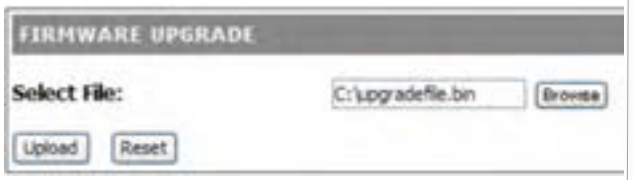


Fig 10. Firmware upgrade by TFTP

Fig 11. Lad Settings via HTTP

Upgrading Firmware by HTTP or TFTP

To upgrade firmware of the DeskPoint Pro via HTTP:

1. Click **Browse** and then select a correct firmware .bin file. The firmware file path will be shown in the Firmware file name text box.
2. Click **Upgrade** to begin the upgrade process.

To upgrade firmware of the DeskPoint Pro via TFTP:

1. Setting TFTP **Server IP** and then type a correct firmware **.bin** file.
2. The firmware file will be shown in the Firmware file name text box.
3. Click **Upgrade** to begin the upgrade process.

Load Settings by HTTP or TFTP

To Load setting of the device via HTTP:

1. Click **Browse** and then select a correct firmware **.dat** file. You have to make sure the file name is the Device's MAC address. The configuration file path will be shown in the Firmware file name text box.
2. Click **Upload** to upload the configuration file to the device.

To Load setting of the device via TFTP:

1. Setting TFTP **Server IP** and then type a correct configure file. The default upload file name is *MACName.dat*.
2. The firmware .dat file will be shown in the Firmware file name text box.
3. Click **Upload** to upload the configuration file to the device.

Fig 12. Load Settings via TFTP

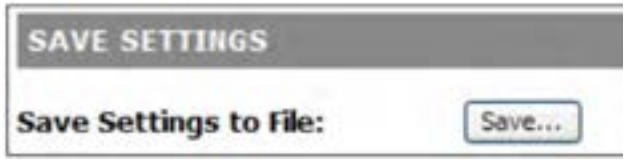


Fig 13. Save the configuration file

Note 1: The procedure may be a little different with different web browsers.

Note 2: Make sure to open “Accept acces requests” in the tftp server.

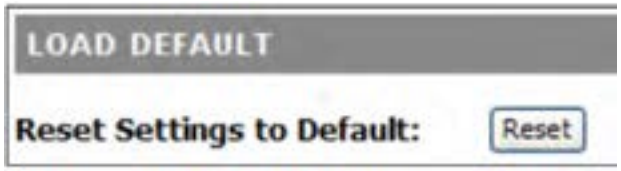


Fig 14. Resetting configuration to Factory Defaults

Fig 15. Restart the system

Save Settings by HTTP or TFTP

To back up configuration of the device via HTTP or TFTP:

1. You’ll be prompted to open or save the configuration file. Click **Save**.
2. The configuration file is named by the DeskPoint Pro’s MAC address. For example, if the DeskPoint Pro’s MAC address is 00-01-02-aa-bb-cc, the configuration backup file should be “000102aabbcc.dat”. Don’t change the configuration file name in the **Save As** dialog box. Select a folder in which the configuration file is to be stored. And then, click Save.

Resetting Configuration to Factory Defaults

Click the **Reset** button resets the device configuration to factory defaults.

WARNING: Check before clicking the **Reset** button before overriding all current configuration setting.

Click the **Reboot** button to restart the device and waiting 40 to 60 seconds. New message will prompt:

Change setting successfully!

Do not turn off or reboot the device during this time.

Please wait 35 seconds…

System Settings

You can change the User Name and Password of Administrator (Manager) in the function.

Web Management – secure and idle timeout

On this page, you could change the Web Management in HTTP, HTTPS or HTTP & HTTPs both. The administrator can view and modify the configuration of the DeskPoint Pro. The new password must be typed twice for confirmation. If you want use SSL to protect and manage the device, you can select HTTPS for Secure management, https default port number is 443 and http is 80.

Fig 20. URL box on IE Browser, use https:// for SSL protection.

The setting specifies how long the idle time during which the WEB administrator connection is maintained during inactivity. The default value is 10 minutes.

Notes: HTTPS (Hyper text Transfer Protocol over Secure Socket Layer) is a URI scheme used to indicate a secure communication such as payment transactions and corporate information systems. HTTPS is not a separate protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. This ensures reasonable protection from eavesdroppers but is weak with man-in-the-middle attacks.

System Tools

Ping

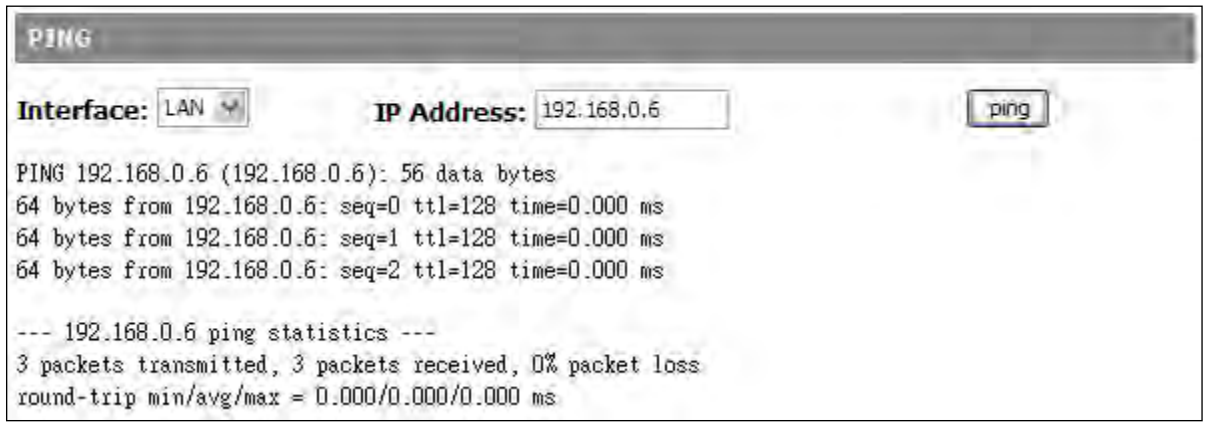


Fig 21. Ping Tool

Fig 16. Manager name and password settings

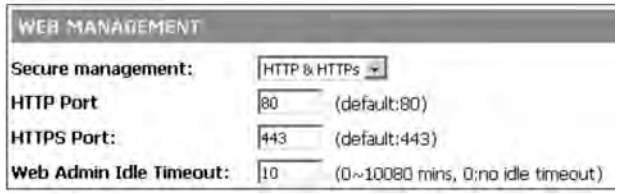


Fig 17. Web Management settings

The function will help you to respond to ping requests from a device on Ethernet or Wide Area Network that are sent to LAN IP.

Arping

Fig 22. Arping Tool

Arping is a function which is similar in function to ping requests from a device on Ethernet that are sent to LAN IP, but it operates using Address Resolution Protocol (ARP) instead of Internet Control Message Protocol.

Traceroute

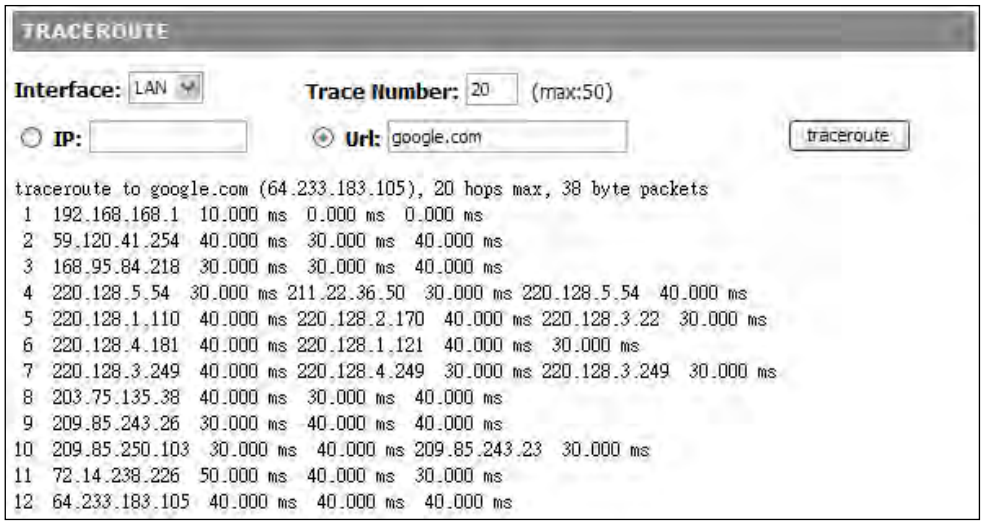


Fig 23. Traceroute Tool

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Traceroute utilizes the IP protocol time to live field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host. This tool is intended for use in network testing, measurement and management. **IP** or **URL** is available. To use URL set IP interface to DHCP. The results show the hop addresses numerically rather than symbolically and numerically.

Time Zone Settings

DeskPoint Pro can maintain the system time by synchronizing with a public time server over the Internet. To schedule a periodic reboot, you can enter the day, hour and min for the system.

NTP Settings

In this section, you can set time manually and enable/disable Daylight Saving Time and synchronization of time upgrading.

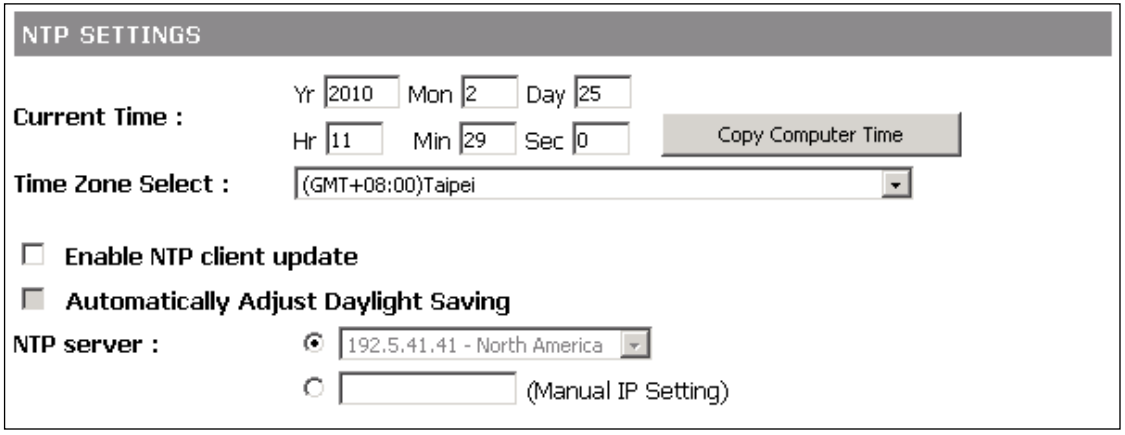


Fig 24. Daylight Saving Time setting

Fig. 25 Periodic Reboot setting

Periodic Reboot

In this section, you can set a time to order the device to reboot itself automatically.

SNMP

SNMP V1 &V2

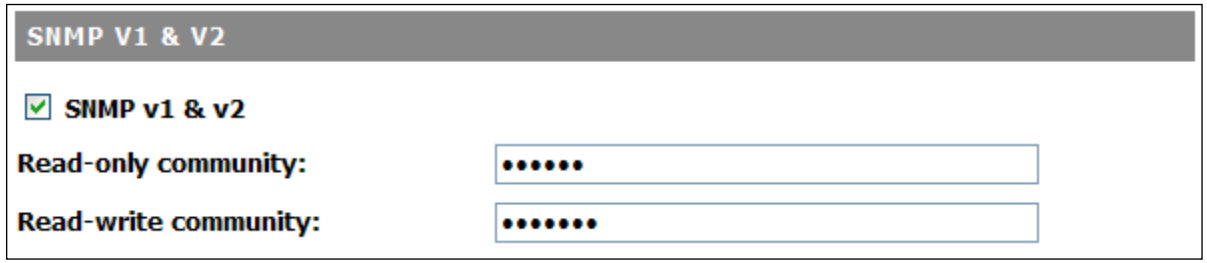


Fig 26. SNMP settings

The DeskPoint Pro can be managed by SNMP (Simple Network Management Protocol) and the SNMP management functionality can be disabled. You can specify the name (used as a *password*) of the read-only and read-write community.

SNMP V3 Settings

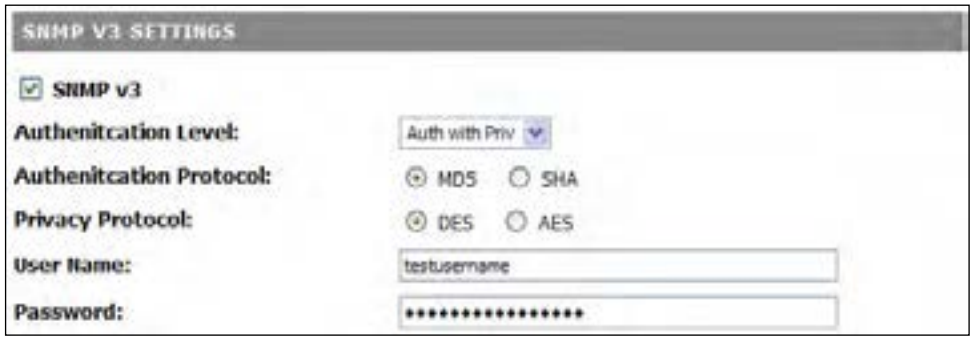
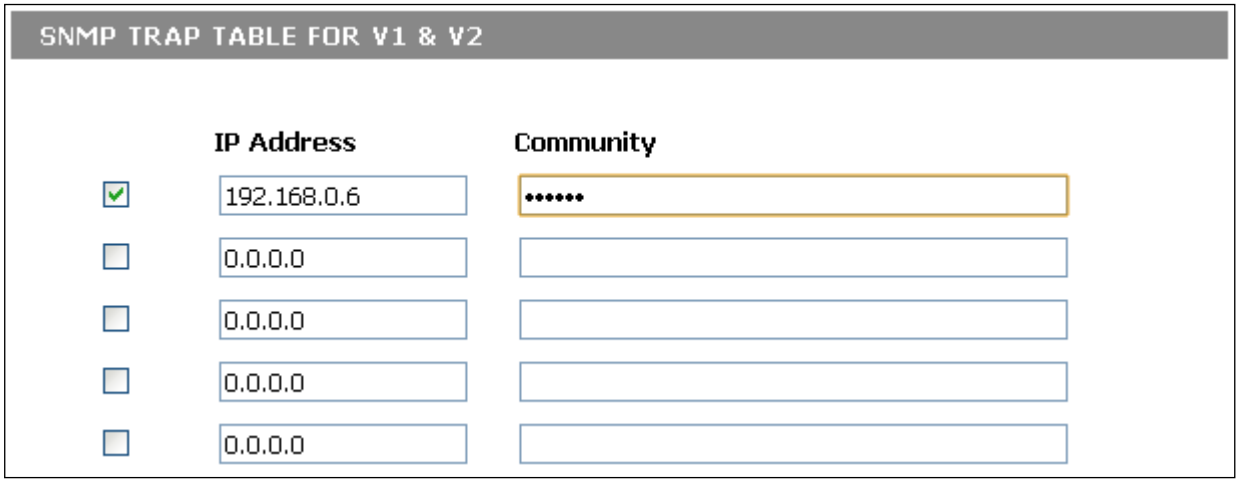


Fig 27. SNMP settings

SNMPv3 primarily added security and remote configuration enhancements to SNMP. There are three modes in the Authentication Level. **No Auth**, **Auth** and **Auth with priv.** Only input the User Name in No Auth mode. Select the Authentication Protocol and apply the user name /password in the Auth Mode. Select the authentication protocol and privacy protocol if choose the Auth with Priv mode.

Authentication Level	Authentication Protocol	Privacy Protocol	User Name	Password
No Auth	X	X	○	X
Auth	○	X	○	○
Auth with Priv	○	○	○	○

SNMP TRAP TABLE FOR V1 & V2



Up to 5 SNMP (Simple Network Management Protocol) traps can be set in the SNMP Trap Table if SNMP V1/V2 is enabled.

To specify a trap target:

1. Type the IP address of the target host.
2. Type the Community for the host.
3. Select the corresponding check box next to the IP address text box.

Configuring TCP/IP Related Settings

LAN

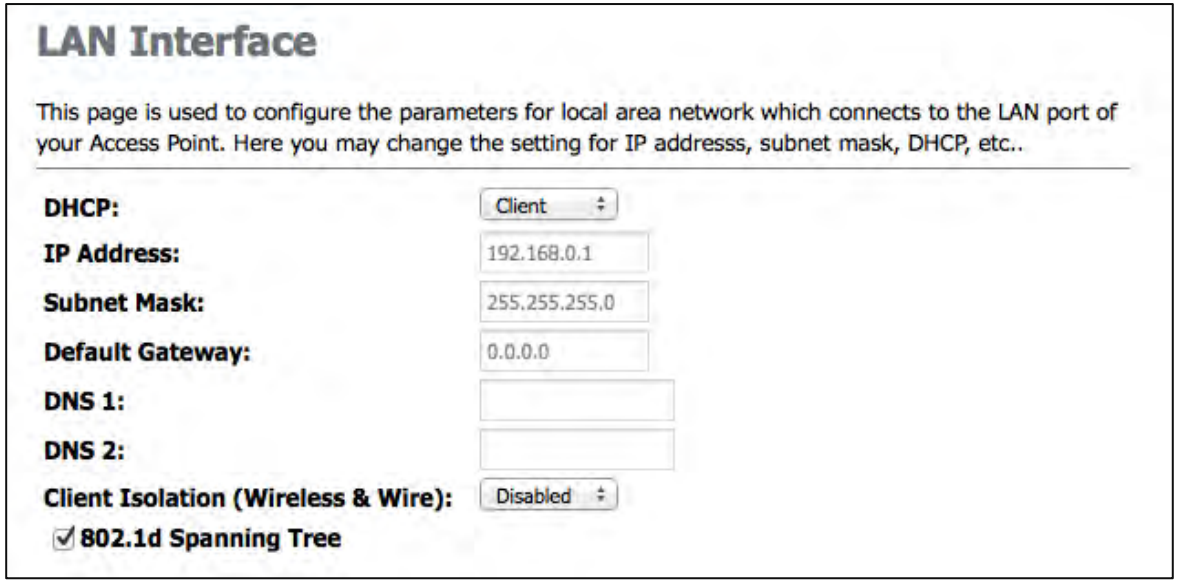


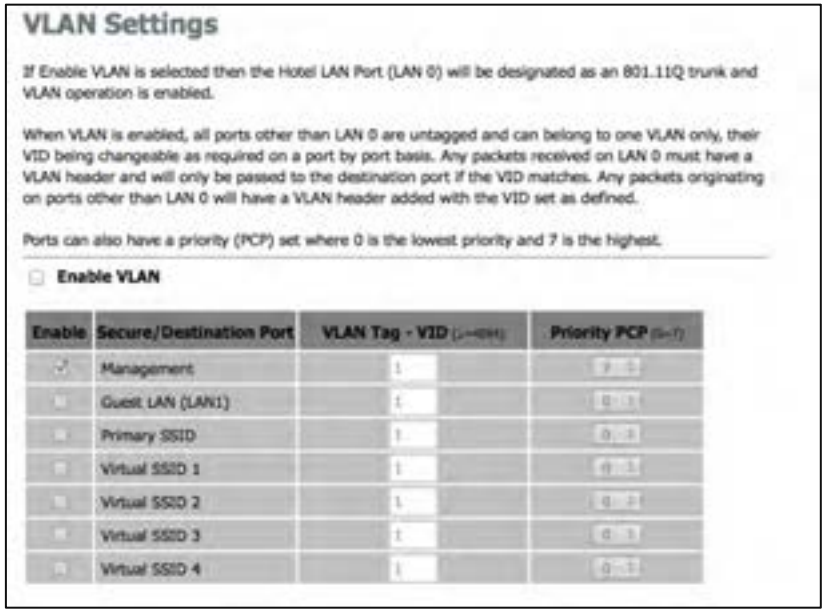
Fig 29. LAN settings

You can either use DHCP or Static IP for your TCP/IP LAN Settings. When manually set the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. Above setting is for static LAN IP, setting the **DHCP Disabled.** If Setting **DHCP Client** mode it mean DeskPoint Pro will automatically obtain an IP address from a DHCP server.

Client Isolation blocks traffic between wired and wireless clients of the DeskPoint Pro. In a hotel environment it is generally desirable to enable this setting to ensure guest privacy. Note however that the DeskPoint Pro will not block traffic between wired and wireless clients connected to different DeskPoint Pro's, this function must be performed by the network infrastructure.

Note: **Spanning Tree Protocol** is an OSI layer-2 protocol that ensures a loop-free topology for any bridged LAN. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

VLAN Tag



When VLAN tagging is enabled then the Hotel LAN port will become an 802.1Q trunk. The Web management (or SNMP), Guest LAN and Primary SSID can all be assigned a VLAN tag to allow the network switch to identify and route tagged connection. If multiple Aps are configured then each additional SSID (AP) can also have it's own assigned VLAN tag. The priority bits of each VLAN can also be assigned to allow the network to prioritise particular VLANs.

4. Configuring IEEE 802.11-Related Settings

Basic Settings

Wireless Basic Settings

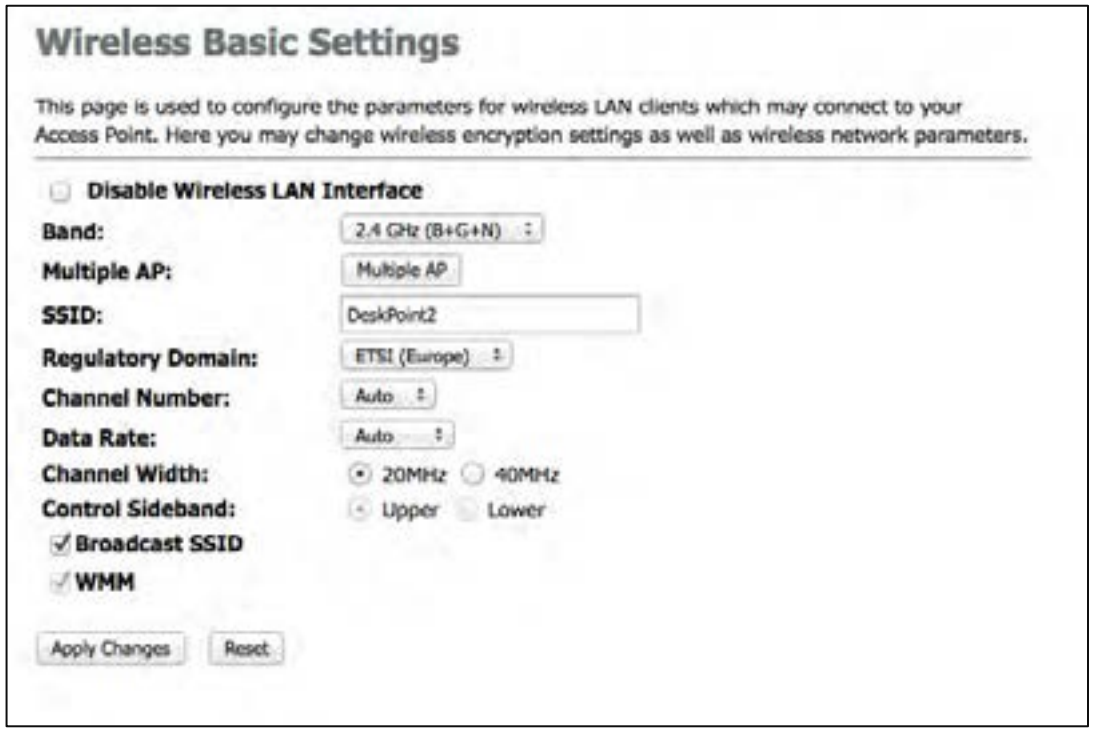


Fig 30. Basic IEEE 802.11 communication Setting of WLAN

The wireless interface can be enabled or disabled. By default it is enabled.

You can choose one **Band** as follows:

- 2.4GHz (B): 802.11b supported rate only.
- 2.4GHz (G): 802.11g supported rate only.
- 2.4GHz (N): 802.11n supported rate only.
- 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.
- 2.4GHz (G+N): 802.11g supported rate and 802.11n supported rate.
- 2.4GHz (B+G+N): 802.11b, 802.11g and 802.11n supported rate.

The default is 2.4GHz (B+G+N) mode.

The DeskPoint Pro can support 4 additional SSIDs. Select this option to enable and configure the basic wireless settings for each virtual SSID (band, SSID, data rate, broadcast SSID and WMM. You can also view the active client list for each SSID.

Since the DeskPoint Pro is also IEEE 802.11b and IEEE802.11g compatible, you can configure the **Date Rate** setting to meet your backwards compatibility needs. If there is RF interference, you may want to reduce the **Data Rate** for more reliable wireless transmission. In most cases, leave the setting to **Auto**.

The number of available **RF channels** depends on local regulations, The regulatory domain is determined by the firmware that is loaded. The SSID of a wireless client computer and the SSID of the DeskPoint Pro must be identical for them to communicate with each other.
Broadcast SSID: Enabled; the DeskPoint Pro will broadcast its SSID to stations. And if disabled: This DeskPoint Pro will not broadcast its SSID to stations. If stations want to connect to this DeskPoint Pro, this it's SSID should be known in advance to make a connection.

Primary Channel	20 MHz	40 MHz Upper			40 MHz Lower		
	blocks	Sec. Ch.	center	blocks	Sec. Ch.	center	blocks
1	1-3	5	3	1-7	Not Available		
2	1-4	6	4	1-8	Not Available		
3	1-5	7	5	1-9	Not Available		
4	2-6	8	6	2-10	Not Available		
5	3-7	9	7	3-11	1	3	1-7
6	4-8	10	8	4-12	2	4	1-8
7	5-9	11	9	5-13	3	5	1-9
8	6-10	12	10	6-13	4	6	2-10
9	7-11	13	11	7-13	5	7	3-11
10	8-12	Not Available			6	8	4-12
11	9-13	Not Available			7	9	5-13
12	10-13	Not Available			8	10	6-13
13	11-13	Not Available			9	11	7-13

Fig 31. Basic IEEE 802.11n channel settings with 40MHz width

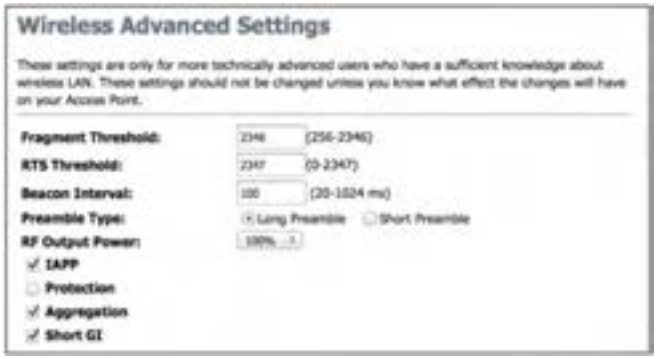


Fig 31. Advanced Setting of WLAN

WMM: The WiFi Multiple Media function is available under 2.4GHz (B), 2.4GHz (G) and 2.4GHz (B+G) band, and is disabled under 2.4GHz (N), 2.4GHz (G+N) and 2.4GHz (B+G+N) band.

11n Setting

The 2.4GHz ISM band is fairly congested. With 802.11n, there is the option to double the bandwidth per channel to 40MHz which results in slightly more than double the data rate.

The specification calls for requiring one primary 20 MHz channel as well as a secondary adjacent channel spaced ±20 MHz away. The primary channel is used for communications with clients incapable of 40 MHz mode. When in 40 MHz mode the center frequency is actually the mean of the primary and secondary channels. Since the Band is selecting 2.4GHz (N) or using any include N mode, the 20MHz/40MHz **channel width**, the channel number be suggested using form 5~11 and auto; Select 20MHz channel width the channel number will be form 1~11 and auto. And Select **Control Sideband** Upper or Lower from pull-down menu.

Advanced Setting

These settings are only for more advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your DeskPoint Pro and the network as a whole.

Advanced settings include Fragment Threshold, RTS Threshold, Beacon Interval, Preamble Type, RF Output Power, IAPP (802.11f support), Protection, Aggregation and Short GI.

Fragment Threshold: Setting for data packet fragmentation threshold, value can be written between 256 and 2346 bytes.

RTS Threshold: Set the RTS Threshold, value can be written between 0 and 2347 bytes.

Beacon Interval: The beacon is a periodic packet the DeskPoint Pro sends out on the air to announce its presence and name (SSID). Beacon Interval represents the amount of time between beacon transmissions. Set the Beacon Interval, value can be written between 20 and 1024 ms.

Preamble Type: Click to select the Long Preamble or Short Preamble support on the wireless data packet transmission.

RF Output Power: To adjust transmission power level.

IAPP: Click to enable or disable the IAPP function.

Protection: Protect 802.11n user priority.

Aggregation: Click to enable or disable the Aggregation function.

Short GI: Click to enable or disable the short Guard Intervals function.

Security

IEEE 802.11 security settings include **None**, **WEP**, **WPA**, **WPA2** and **WPA2 Mixed**. The default setting is **None** (Open System). In a hotel setting a separate authentication system is generally deployed and the DeskPoint Pro would be configured without any security settings. If there is not a separate authentication system you should consider the use of WEP, WPA, WPA2 or WPA2 Mixed to prevent any unauthorized access. In this instance both the guest PC and the DeskPoint Pro must have the same settings for security.

Note: When the security mode is set to Open System, no authentication or data encryption will be performed by the DeskPoint Pro. Also note, that when Multiple AP's have been configured you will need to configure the security settings that apply to the Primary SSID and any enabled virtual SSIDs.

Open System - No authentication, no data encryption.

Static WEP - WEP (Wired Equivalent Privacy) keys must be manually configured.

WPA-Personal (WPA-PSK) - Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you have to specify the Pre-shared key, which will be used by the TKIP engine as a *master key* to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

WPA2-Personal (WPA2-PSK) - The advanced protocol, certified through Wi-Fi Alliance's WPA2 program, implements the mandatory elements of 802.11i. WPA2 is an improvement on the WPA-PSK standard, and is simply using a shared password for access to your network. Only users with this password can access your network.

WPA-Enterprise (WPA) - This is a full WPA mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The DeskPoint Pro is highly secured in this mode.

WPA2-Enterprise (WPA2) - This is a full WPA2 mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The DeskPoint Pro is highly secured in this mode.

WPA-Mixed - This is a full WPA2 mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The DeskPoint Pro is highly secured in this mode.

WEP

WEP is not available if 802.11n is set. According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, *Shared Key* authentication is used if WEP data encryption is enabled. In rare cases, *Open System* authentication may be used when WEP data encryption is enabled. The **Authentication algorithm** setting is provided for better compatibility with wireless client computers with various WLAN network adapters. There are three options available, including *Open System*, *Shared Key*, and *Auto*.

Fig 33. WEP settings

***Note**: The number of characters if the Pre-Shares Key setting must be at least 8 and can be up to 63.*

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the local device side to the remote device side.

- Key Length: select key length 64-bit or 128-bit.
- Key Format: Select the Hex (10 characters) or ASCII (5 characters).
- Hexadecimal (WEP 64 bits): 10 Hex characters (0~9, a~f).
- Hexadecimal (WEP 128 bits): 26 Hex characters (0~9, a~f).
- ASCII (WEP 64 bits): 5 ASCII characters (case-sensitive).
- ASCII (WEP 128 bits): 13 ASCII characters (case-sensitive).

Key Setting: Enter the key in the key setting field.

In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1x functionality is enabled. See Section 4.8.3.5 for more information about IEEE 802.1x and RADIUS.

WPA

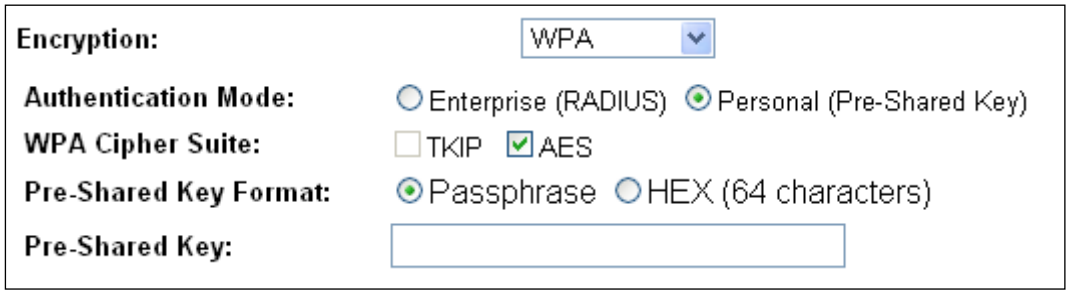


Fig 34. WPA settings

Authentication Mode: Select Enterprise (RADIUS) or Personal (Pre-Shared Key) mode.

WPA Cipher Suite: here supported AES only.

Pre-Shared Key Format: There are two formats for choosing to set the pre-shared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.

Pre-Shared Key: Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

WPA2

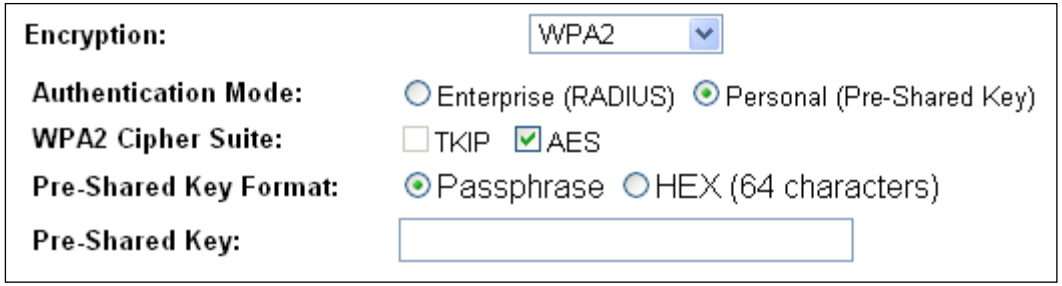


Fig 35. WPA2 settings

Authentication Mode: Select Enterprise (RADIUS) or Personal (Pre-Shared Key) mode.

WPA2 Cipher Suite: supports AES only.

Pre-Shared Key Format: There are two formats for choice to set the Pre shared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.

Pre-Shared Key: Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

WPA-Mixed

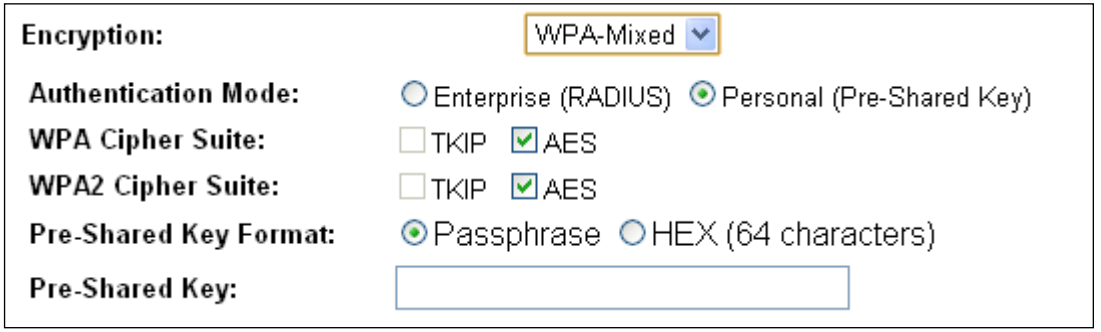


Fig 36. WPA-Mixed settings

Authentication Mode: Select Enterprise (RADIUS) or Personal (Pre-Shared Key) mode.

WPA Cipher Suite: here supported AES only.

WPA2 Cipher Suite: here supported AES only.

Pre-Shared Key Format: There are two formats for choice to set the Preshared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.

Pre-Shared Key: Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

Radius

IEEE 802.1x Port-Based Network Access Control is a standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its

mobile users' access to its wireless LANs. Before being granted access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her user name and password or digital certificate to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

An IEEE 802.1x-capable wireless access point and its RADIUS server(s) share a secret key so that they can authenticate each other. RADIUS server is needed if IEEE 802.1x functionality is enabled.

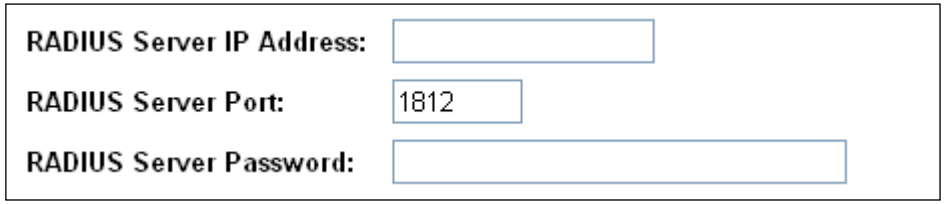


Fig 37. RADIUS settings

RADIUS Server IP Address: Enter the RADIUS Server's IP Address provided by your ISP.

RADIUS Server Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.

RADIUS Server Password: Enter the password that the DeskPoint Pro shares with the RADIUS Server.

5. Viewing Status

Network Status Table

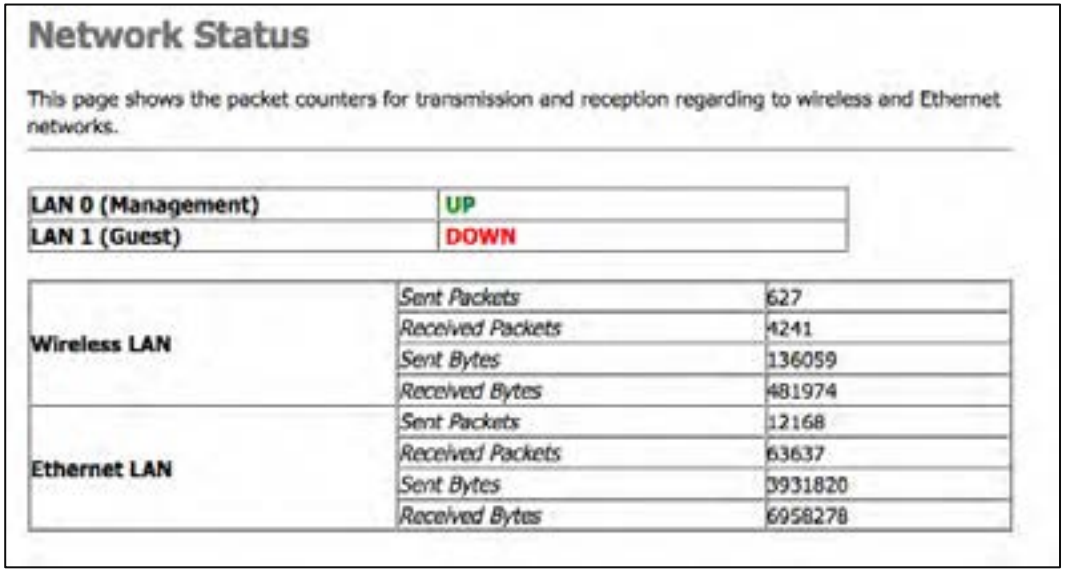


Fig 38. Wireless/Ethernet Network Status Table

On this page, the Ethernet and wireless transport status are shown.

Syslog

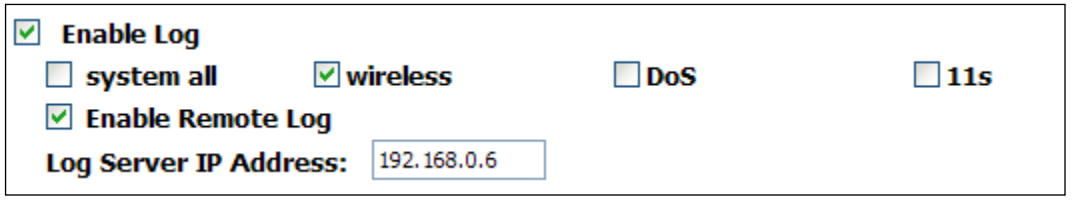


Fig 39. System Log

System events can be logged to the on-board RAM of the Deskpoint Pro (**Local log**) or **Log Server IP Address** to a remote Syslog server, respectively. See the SNMP section for more information about SNMP trap settings. Set the IP address of the Syslog server in the **Syslog server IP address** text box.

The system events are divided into the following categories:

Enable Log Check to enable logging function.

System all Activates all logging functions.

Wireless Only logs related to the wireless LAN will be recorded.

DoS Only logs related to the DoS protection will be recorded.

Enable Remote Log Only logs related to the Remote control will be recorded.

Log Server IP address Only logs related to the server will be recorded.

Network Status

MAC Address	Mode	Tx Packet	Rx Packet	Current Tx Rate (Mbps)	Power Saving	Expired Time (s)	RSSI	Channel Width
00:e0:4c:72:00:01	11n	1286	1732	108	no	300	58 (63 56)	40M
00:0e:35:ae:c1:96	11g	30	109	54	no	289	55 (0 0) 6)	20M

Fig 40. Wireless Clients Status

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1x authenticated), number of bytes it has send, number of bytes it has received, and the time of its last activity, is shown.

6. Technical Support

For North and South American 24/7 Technical Support

Toll-Free: 1 877 835 3232 x306 (in US and Canada)

Main: 1 775 232 5044

Email: ric.jones@us.teleadapt.com

For EMEA Technical Support

Main: +44 1923 810235

Email: info@teleadapt.com

For APAC Technical Support

Main: +82 10 8566 0809

Email: dg.hong@teleadapt.com

Appendix A: Default Settings

Setting Name	Default Value
Global	
User Name	root
Password	root
IEEE 802.11G	
Regulatory Domain	Firmware dependent
Channel Number	Auto
SSID	DeskPoint2
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	100%
MAC Address	Refer to the label on the bottom of the housing
Data Encryption	Disabled
Wireless Client Isolation	Disabled
LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Client Isolation	Enabled
MANAGEMENT	
System Log	Local Log
SNMP	Disabled
SNMP Read-only community	public
SNMP Read-write community	private


teleadapt
Keeping Your World Connected™