SILVERNET

MICRO

LITE

MAX

BASE

Pro RANGE

User Manual

Version 1.3 (24/07/2014)

Table of Contents

Introduction

This User Guide describes the firmware version 2.30.1 which is integrated into all Pro Range 95 and 240 products provided by SilverNet Ltd.

Supported Products

This manual covers all Pro 95 and Pro 240 products listed below:

- MICRO 95
- LITE 95
- MAX 95
- BASE 95
- LITE 240
- MAX 240
- BASE 240
- ACCESS 240

For more information, visit **www.silvernet.com**

Pro Range Network Modes

The SilverNet Pro Range supports the following network modes:

- Transparent Bridge mode (layer 2)
- Router Mode

Pro Range Wireless Modes

The Pro Range supports the following wireless modes:

- Station
- Station WDS
- Access Point
- Access Point WDS
- Repeater
- Repeater WDS
- Wireless Adapter

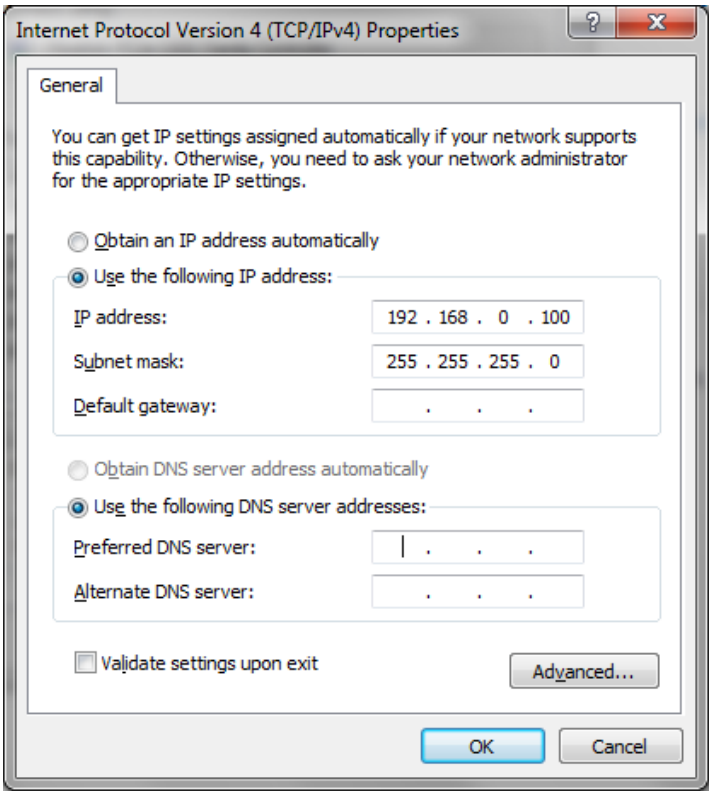
System Requirements

- Windows XP, Windows Vista, Windows 7, Windows 8, Linux, or Mac OS X
- Web Browser: Mozilla Firefox, Apple Safari, Google Chrome, or Microsoft Internet Explorer 8 (or above)

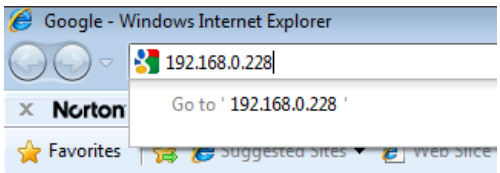
Getting Started

To access the Pro Range Configuration Interface, perform the following steps:

1. Configure the Ethernet adapter on your computer with a static IP address on the 192.168.0.x subnet (for example, IP address: *192.168.0.100* and subnet mask: *255.255.255.0*



2. Launch your web browser and enter the default IP address of your device in the address field. Press **Enter** (PC) or **Return** (Mac).
Pro Range products 192.168.0.229/192.168.0.228



If the unit has reset, it will go to the default IP address of 192.168.168.1. You will need to change your Ethernet adapter IP address to 192.168.168.x subnet.

3. Enter **admin** in the *Username* field and **password** in the *Password* field, and click **Login**.

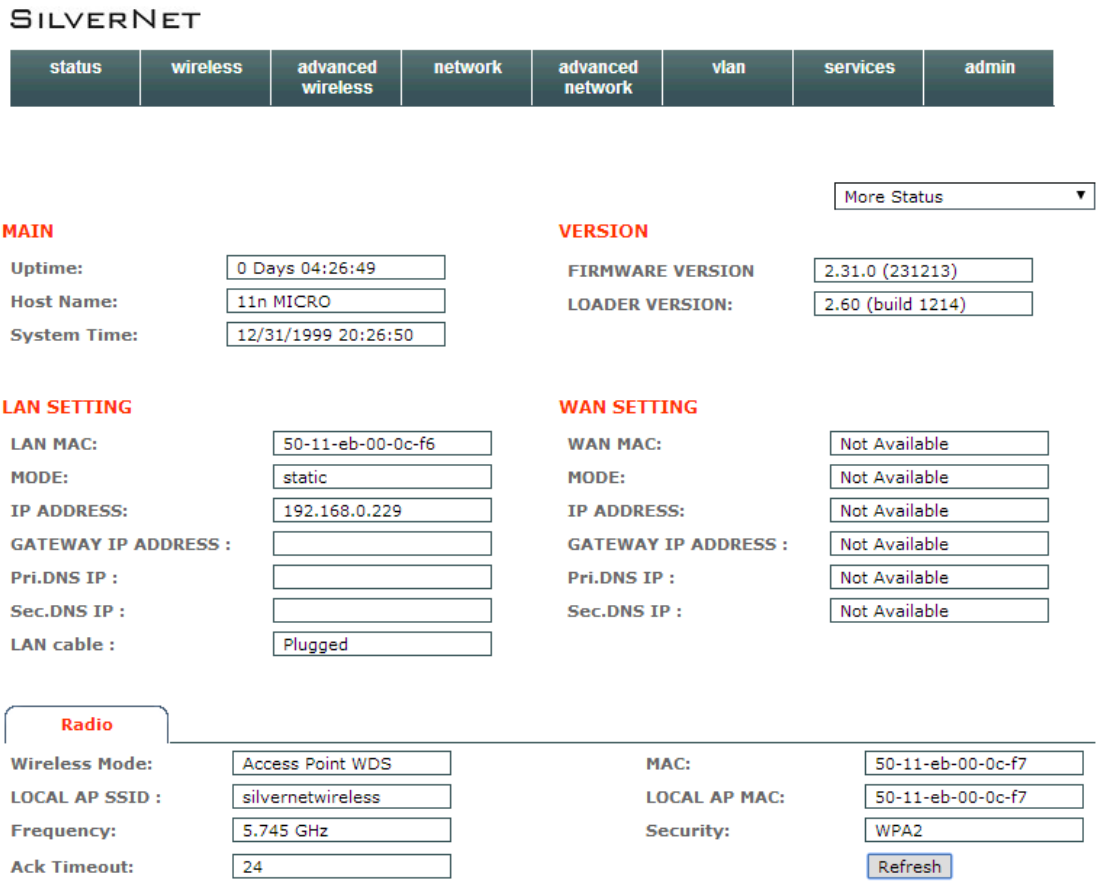
Navigation

The Pro Range Configuration Interface contains eight main tabs, each of which provides a web-based management page to configure a specific aspect of the SilverNet device:

• **Status** The **"Status Tab"** displays device status, statistics, and network monitoring links.
• **Wireless** The **"Wireless Tab"** configures basic wireless settings, including the wireless mode, Service Set Identifier (SSID), 802.11 mode, channel and frequency, output power, data rate module, and wireless security.
• **Advanced Wireless** The **"Advanced Wireless Tab"** provides more precise wireless interface controls, including advanced wireless settings, distance settings, and signal LED thresholds.
• **Network** The **"Network Tab"** configures the network operating mode; Internet Protocol (IP) settings, DHCP settings and bandwidth control.
• **Advanced Network** The **"Advanced Network Tab"** provides more precise wireless interface controls when the operating mode is changed to **router**. This includes NAT setup, port forwarding and firewall setup.
• **VLAN** The **"VLAN Tab"** configures the VLANs settings for both the Ethernet and the radio.
• **Services** The **"Services Tab"** configures system management services: Ping Watchdog, Simple Network Management Protocol (SNMP), servers (web, SSH, Telnet), Network Time Protocol (NTP) client, Spanning Tree Protocol (STP) and system log.
• **Admin** The **"Admin Tab"** controls administrator accounts management, firmware update, and configuration backup.

Status Tab

The *Status* tab displays a summary of the link status information, current values of the basic configuration settings (depending on the operating mode), network settings and information, and traffic statistics.



Main

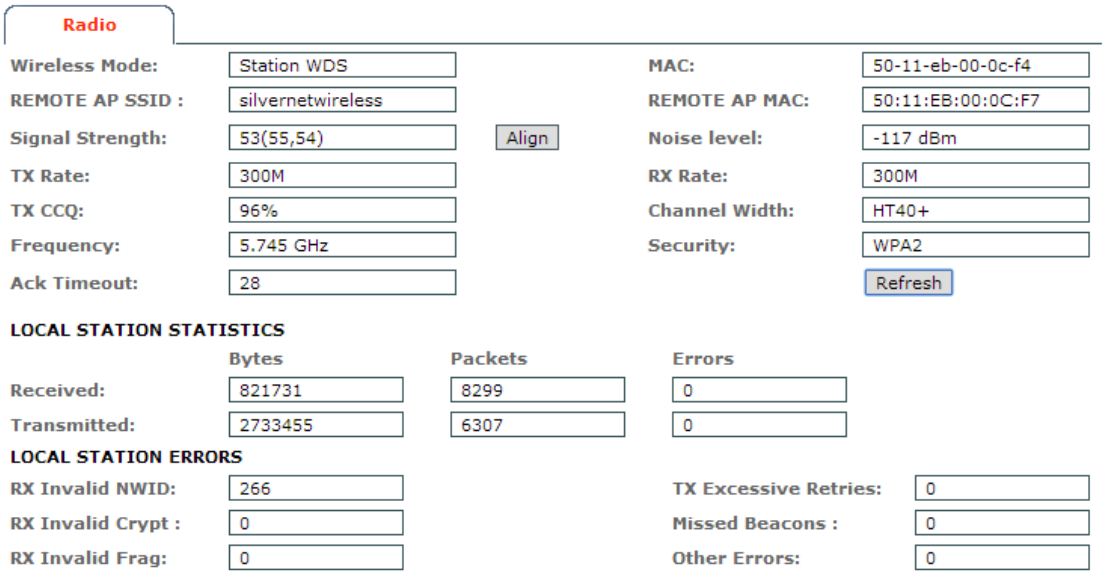
Uptime This is the total time the device has been running since the last reboot or software upgrade. The time is displayed in days, hours, minutes, and seconds.
Host Name Displays the customizable name or identifier of the device. The host name is also displayed in SilverView.
System Time Displays the current system date and time. The date and time are displayed in DAY-MONTH-YEAR HOURS:MINUTES:SECONDS format. The system date and time is retrieved from the Internet using NTP (Network Time Protocol). The NTP Client is disabled by default on the *Services* tab. The device doesn't have an internal clock, and the date and time may be inaccurate if the NTP Client is disabled or the device isn't connected to the Internet.

Version

Firmware Version Displays the SilverNet unit's software version.
Loader Version Displays the SilverNet unit's boot loader version.

LAN/WAN settings

LAN MAC Displays the MAC address of the device as seen on the LAN.
WAN MAC Displays the MAC address of the device as seen on the WAN.
Mode Displays the network operating mode.
IP address Displays the current IP address of the unit.
Gateway Address Displays the gateway address assigned by an external DHCP server connected to the WAN interface.
Primary DNS/Secondary DNS IP The Domain Name System (DNS) is an Internet "phone book" that translates domain names to IP addresses. These fields identify the server.
LAN cable Indicates the current status of the LAN Ethernet port connection. This can indicate that a cable is not plugged into a device or there is no active Ethernet connection.



Radio

Wireless Mode Displays the operating mode of the radio interface. The Pro Range supports seven operating modes:

- Station
- Station WDS
- Access Point
- Access Point WDS
- Repeater
- Repeater WDS
- Wireless Adapter

Local/Remote AP SSID In *Access Point* (WDS) mode, this displays the SSID of the device. In *Station* (WDS) mode, this displays the SSID of the AP the device is associated with.

Frequency Displays the operating frequency of the device.

Ack Timeout The ACK timeout specifies how long the device should wait for an acknowledgement from another device, confirming it has received a packet before it concludes that there has been an error and resends the packet. Changing the distance value will change the ACK (Acknowledgement) timeout accordingly.

Signal Strength (Available in *Station* (WDS) mode only.)

Displays the received wireless signal level. Use the align button and adjust the device antenna to get a better link.

(35 to 45 dBm) is recommended for stable links.

TX Rate (Available in *Station* (WDS) mode only.)

Displays the devices current data transmission (TX) rates or "radio speed".

Transmit CCQ This index evaluates the wireless Client Connection Quality (CCQ). The level is based on a percentage value for which 100% corresponds to a perfect link state.

MAC This displays the MAC address of the device.

Local/Remote AP MAC In *Access Point* (WDS) mode, this displays the MAC address of the device. In *Station* (WDS) mode, this displays the MAC address of the AP the device is connected to.

Security Displays the wireless security method being used on the device. If *None* is displayed, then wireless security has been disabled.

Noise Level Displays the noise level (in dBm)

RX Rate (Available in *Station* (WDS) mode only.)

Displays the devices current data reception (RX) rate

Channel Width Displays the spectral width of the radio channel. You can use this option to control the bandwidth consumed by your link. Using higher bandwidth increases throughput. Using lower bandwidth reduces throughput. Channel widths available are **5 MHz**, **10 MHz**, **20 MHz**, **20/40 MHz**.

Local AP/Station Statistics

Received Bytes Displays the total amount of data (in bytes) received during the connection.

Received Packets Displays the total amount of packets received

Received Errors Displays the number of receive errors

Transmitted Bytes Displays the total amount of data (in bytes) transmitted during the connection.

Transmitted Packets Displays the total amount of packets transmitted

Transmitted Errors Displays the number of transmit errors

Local AP/Station errors

Rx invalid NWID Displays the number of packets received with a different NWID or ESSID (packets which were destined for another access point).

Rx Invalid Crypt

Displays the number of transmitted and received packets which were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid wireless security settings.

Rx Invalid Frag

Displays the number of packets missed during transmission and reception.

Tx Excessive Retries

Displays the number of packets which failed to be delivered to the destination. Undelivered packet are retransmitted a number of times before an error occurs.

Missed beacons

Displays the number beacons (management packets sent at regular intervals by the Access Point) which were missed by the client. This can indicate that the wireless client is out of range.

Other errors

Displays the total number of transmitted and received packets that were lost or discarded for other reasons.

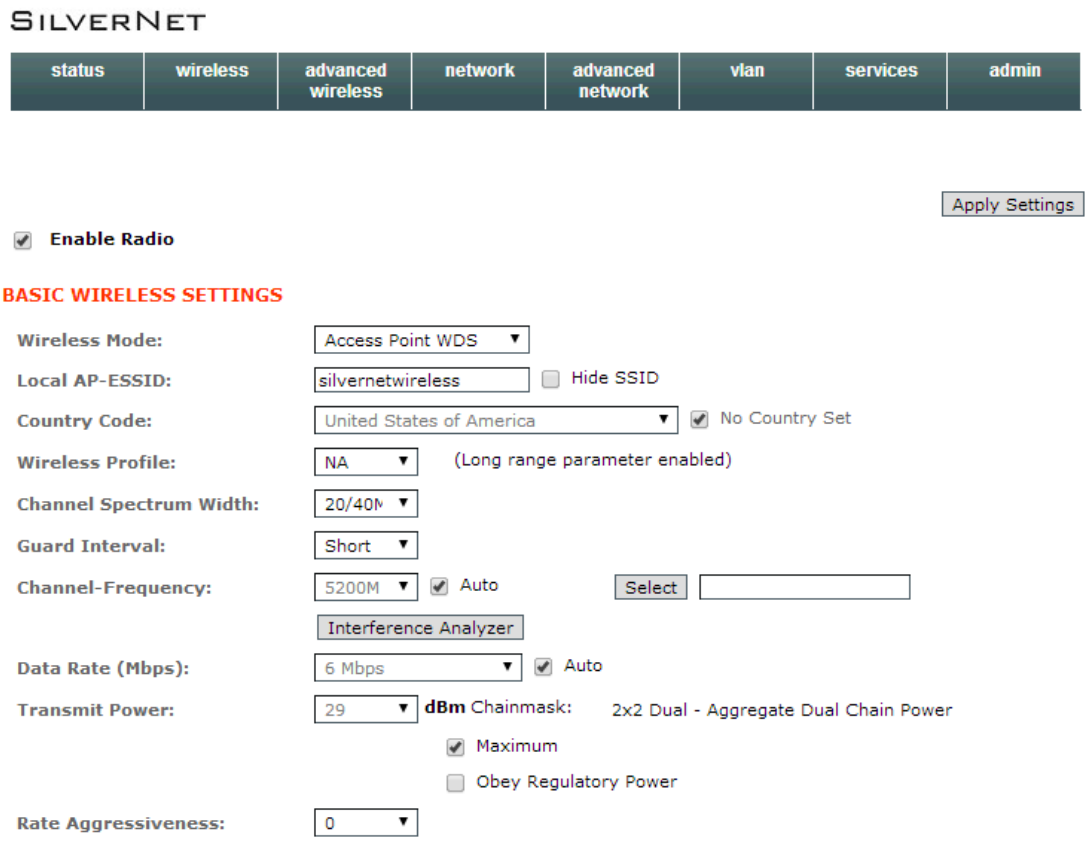
More Status

The "More Status" drop down box contains some useful tools and additional status pages. These are:

- **Ping Utility** – a ping tool to test the connectivity between devices.
- **ARP Table** display a list of MAC addresses of the connected devices
- **Bridge Table** display a list the devices connect to the bridge interface
- **DHCP Active Lease Table** display a list of IPs addresses leased to all computers.

Wireless Tab

The *Wireless* tab contains everything needed to set up the wireless part of the link. This includes SSID, channel and frequency settings, device mode, data rates, and wireless security.



Apply Settings To apply any settings to the radio, click **Apply Settings** Once you have done this it will ask you to either Save or Discard any changes To immediately save your changes, click **Save**. To cancel your changes, click **Discard**.

Basic Wireless Settings

Wireless Mode Displays the operating mode of the radio interface. The Pro Range supports seven operating modes:

- Station
- Station WDS
- Access Point
- Access Point WDS
- Repeater
- Repeater WDS
- Wireless Adapter

Station If you have a client device to connect to an AP, configure the client device as *Station* mode.
The SSID of the AP is used, and it forwards all the traffic to/from the network devices to the Ethernet interface. This mode translates all the packets that pass through to its own MAC address, thus resulting in a lack of transparency.
Station WDS This mode is used to create a transparent bridge and can be connected to a device running in Access Point WDS mode.
Access Point If you have a single device to act as an AP, configure it as *Access Point* mode. The device functions as an AP that connects multiple client devices
Access Point WDS This mode connects to a device running Station WDS mode. It is used to create a transparent bridge.

In most cases, we recommend that you use WDS because it enables transparent Layer 2 traffic. The WDS protocol is not defined as a standard, so there may be compatibility issues between equipment from different vendors.

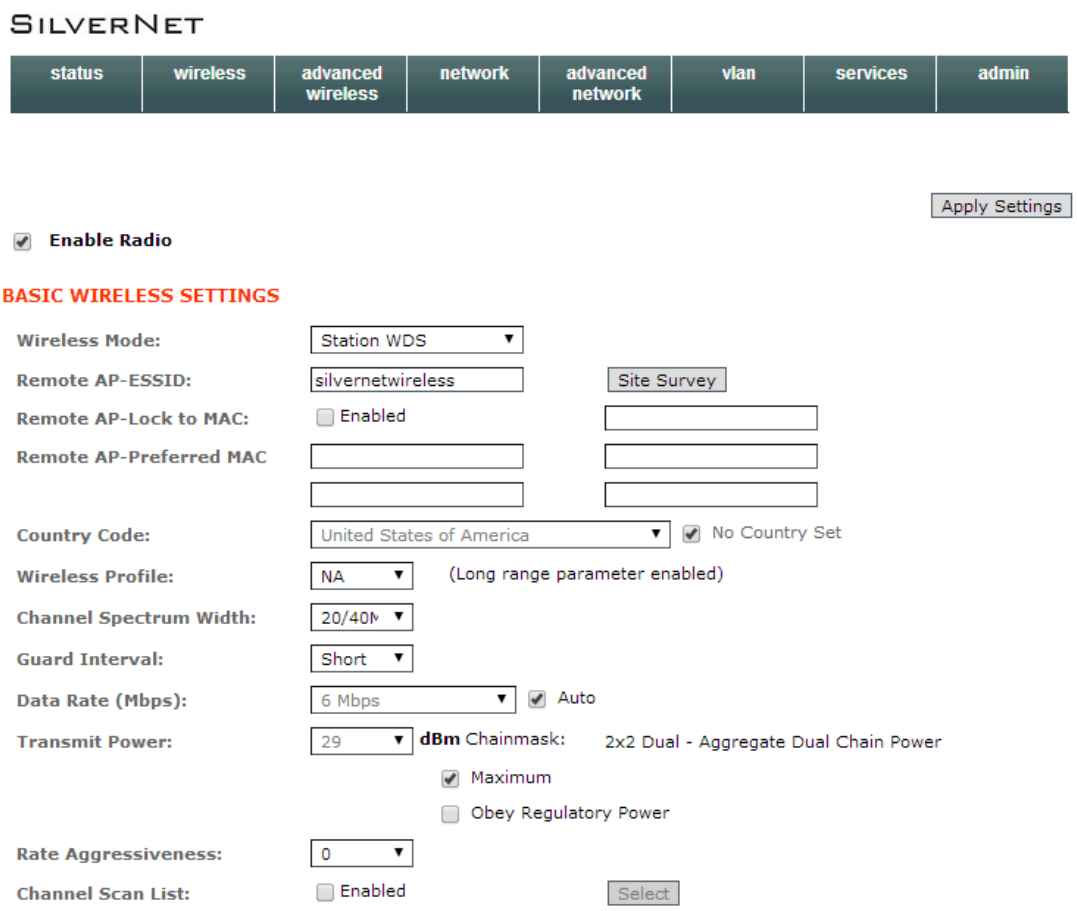
Repeater Mode In this mode the device acts as a relay for network signals on the network by regenerating the signals it receives, and retransmitting them to the main network infrastructure.
Repeater WDS Mode Repeater WDS Mode is used mainly to extend the wireless range and coverage of the wireless network allowing access and communications over places generally difficult for wireless clients to connect to the network.

Repeater WDS requires the access point to be setup in Access Point WDS mode to work. The Repeater WDS must first link up with an Access Point WDS, and then it can link up with a Station WDS. It acts as an extension to the link and you can add more Repeaters as necessary.

Local AP-ESSID If the device is operating in *Access Point* or *Access point WDS* mode, specify the wireless network name or SSID (Service Set Identifier) used to identify your WLAN. All the client devices within range will receive broadcast messages from the AP advertising this SSID. If the device is operating in *Station* mode, specify the SSID of the AP the device is to connect to.
Hide SSID Once checked, this will disable advertising the SSID of the access point in broadcast messages to wireless stations. This option is only available in Access Point, Access Point WDS and Repeater WDS mode.

Site Survey This is **only available in Station/Station WDS mode**. Site Survey will search for the available wireless networks in range on all the supported channels and will allow you to select one for association. If the selected network uses encryption, you'll need to set up the security parameters in the wireless security section. Click Scan to re-scan for the Access Points in range. Select the Access Point from the list and click close this window. Site Survey channel scan list can be modified using the Channel Scan List control.
Remote AP – Lock to MAC This option will make the device only connect to this access point. This is important when connection is Point-to-Point operation as the Station will not look for other Access Points to associate with.
Remote AP - Preferred MAC Enter the preferred MAC address of the access point you want device to connect when it first starts-up. Up to max of 4 MAC addresses can be entered. Priority is from top to bottom. In the event that all preferred MAC addresses are not available, the device will then pick the matching SSID access point with the strongest signal.

Country Code Each country has their own power level and frequency regulations. To ensure the device operates under the necessary regulatory compliance rules, you must select the country where your device will be used. The IEEE 802.11 mode, channel and frequency settings, and output power limits will be tuned according to the regulations of the selected country.
Channel Width Displays the spectral width of the radio channel. You can use this option to control the bandwidth consumed by your link. Using higher bandwidth increases throughput. Using lower bandwidth reduces throughput. Channel widths available are **5 MHz**, **10 MHz**, **20 MHz**, **20/40 MHz**.
Guard Interval This is the Guard band between packets. For long distant connections, select Long to give better performance.
Channel – Frequency The default, Auto, allows the device to automatically select the frequency. You can specify a frequency from the drop-down list. The frequency range available depends on the country you select in Country Code. Some countries have DFS regulations which may affect and delay the device when attempting to establish a connection. It can take up to 15 minutes to connect.



Data Rate Data Rates consist of both the legacy rates and the MCS (Modulation Coding Scheme – Only for 802.11n) rates.

- 6 – 54Mbps are Legacy Rates
- MCS0 to MCS7 are 802.11n rates, which uses only 1 stream.
- MCS8 to MCS15 are 802.11n rates, which uses 2 streams.

When left on **auto** the data rate will follow an advanced rate algorithm that takes into account the amount of errors at that data rate and fine tunes to the best data rate it can use.

Transmit Power The maximum transmit power displayed is determined by the country code and the maximum transmit power of the radio. .

Rate Aggressiveness There are 2 scenarios where the Rate Aggressiveness is useful.

1. When the Environment might be noisy (Interference).
2. When environment is free of interference

For Scenario 1, you can select from -1, -2, or -3. This will lower the throughput but increase the power.

For scenario 2, you can select from +1, +2, +3. This will increase the transmit rate and may improve throughput.

Channel Scan List This restricts scanning to only the selected frequencies. The benefits are faster scanning as well as filtering out unwanted APs in the results. The Site Survey tool will look for APs in selected frequencies only.

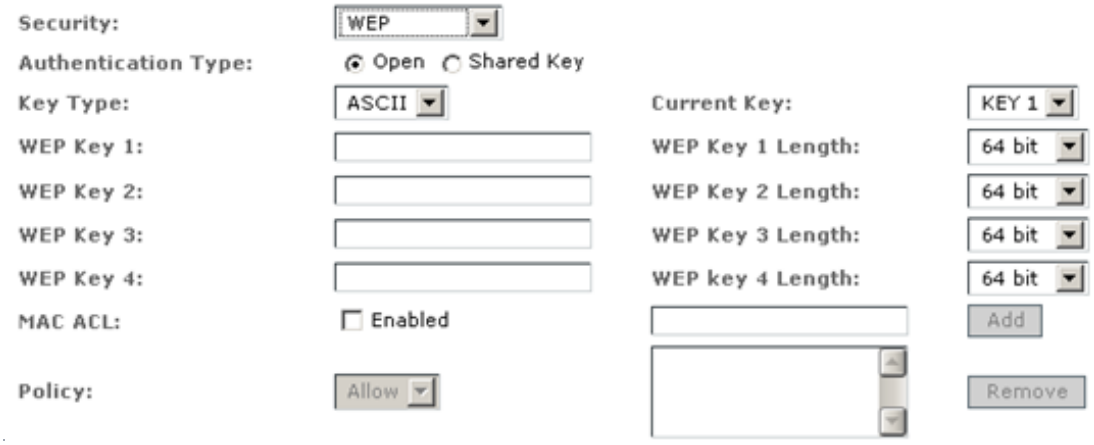
Wireless Security

All the wireless security settings are set under this section.
The operation of the Keys is the same for ALL the Wireless modes.

Security The Pro 95 range supports the following wireless security methods:

None If you want an open network without wireless security, select **none**. You still have the option of using RADIUS MAC authentication and MAC ACL.
WEP WEP (Wired Equivalent Privacy) is the oldest and least secure security algorithm. Use WPA or WPA2 security methods when possible.
WPA WPA (Wi-Fi Protected Access) was developed as a stronger encryption method than WEP.
WPA-TKIP WPA (Wi-Fi Protected Access) security mode with TKIP (Temporal Key Integrity Protocol) support only. TKIP uses the RC4 encryption algorithm. There is a performance limitation to using TKIP, so we recommend using AES.
WPA-AES WPA security mode with AES (Advanced Encryption Standard) support only. AES is also known as CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which uses the AES algorithm.
WPA2 WPA2 was developed to strengthen wireless encryption security and is stronger than WEP and WPA.
WPA2-TKIP WPA2 security mode with TKIP support only. TKIP uses RC4 encryption algorithm. There is a performance limitation to using TKIP, so we recommend using AES.
WPA2-AES WPA2 security mode with AES support only.
This is the strongest security option available. If all of the wireless devices on your network support this option, we recommend that you select it.

WEP



Note: Operating with WEP security will limit AP to maximum wireless link speed of 54Mbps only.

Authentication Type

Open Authentication (Default) No authentication. We recommend to use this option over shared authentication.

Shared Authentication May not be compatible with all Access Points. Not recommended.

Key Type **HEX** or **ASCII** option specifies the character format for the WEP key if WEP security method is used.

Current Key Specify the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used.

WEP Key WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used.

WEP Key Length 64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The 128-bit option will provide a higher level of security.

WPA/WPA2 Authentication

The configuration options are the same for all of the WPA and WPA2 options. WPA2-AES is the strongest security method. If all of the wireless devices on your network support this option, we recommend that you select it.

WPA Authentication Specify one of the following WPA key selection methods:

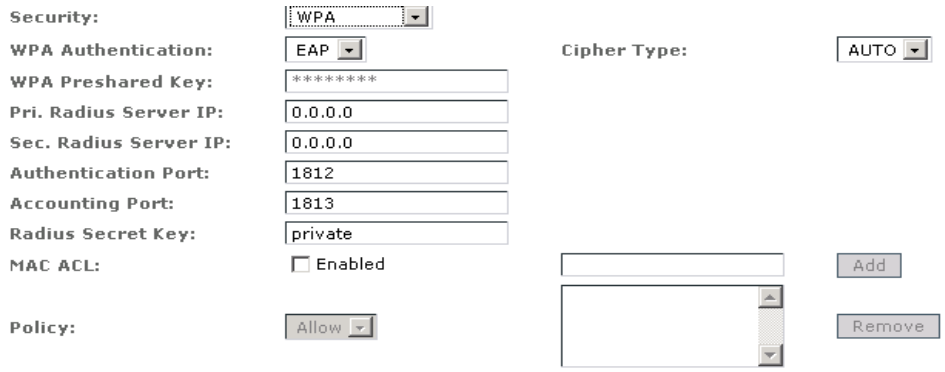
- **PSK** Pre-shared Key method (selected by default).
- **EAP** EAP (Extensible Authentication Protocol)

Cipher Type Specify which of the following to use:

- **TKIP** - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.
- **AES** - Advanced Encryption Standard (AES) algorithm. (**default**)

Pre-shared Key This option is available when **WPA** or **WPA2**, with **PSK** is selected. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

WPA/WPA2 with EAP

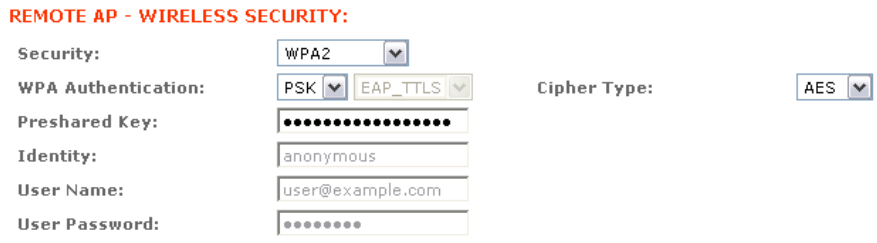


Primary Radius Server IP Enter the Primary Radius Server IP address.
Secondary Radius Server IP Enter the Secondary Radius Server IP address.
Authentication Port Enter the Authentication Port number of the Radius Server. Default is 1812.
Accounting Port Enter the Accounting Port number of the Radius Server. Default is 1813.
Radius Secret Key Enter the Secret Key of the Radius Server. The device uses this key to authenticate itself with Radius Server.

MAC ACL The MAC address Access Control List (ACL) lets you allow or deny clients connectivity to the device. When enabled, you have the following options:
Select a Policy:

- **Allow** Wireless clients on the list can access the device. Any wireless client that is not on the list is denied access to the device.
- **Deny** Wireless clients on the list are denied access to the device. Any wireless client that is not on the list can access the device.

In Station mode you will have the following options for EAP

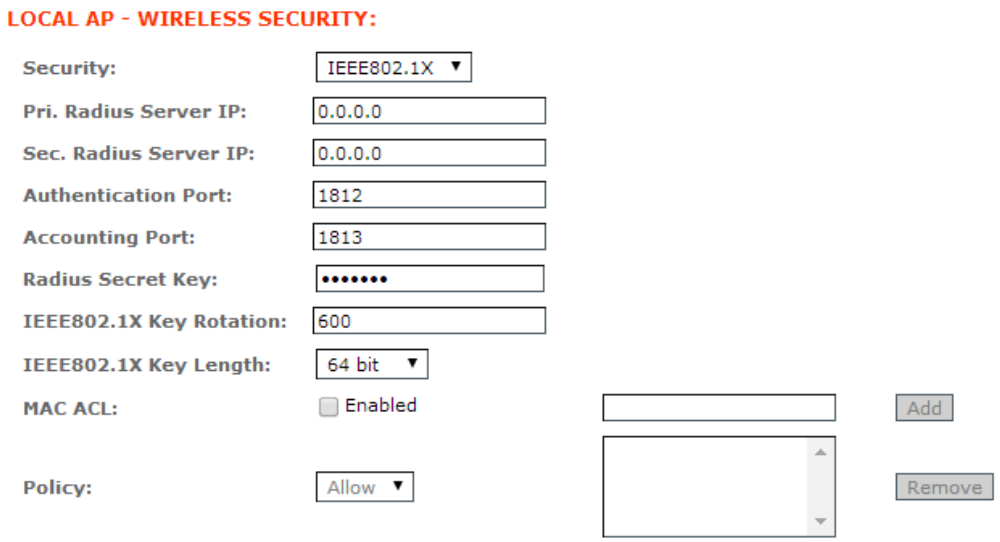


Identity Identification credential used by the WPA-supplicant for EAP authentication.
User Name Identification credential used by the WPA-supplicant for EAP tunnelled authentication in unencrypted form.
User Password Password credential used by the WPA-supplicant for EAP authentication

IEEE802.1x Settings

The operation of the Keys is the same for ALL the modes.

Note: Operating with IEEE802.1x security will limit AP to maximum wireless link speed of 54Mbps only.



Primary Radius Server IP Enter the Primary Radius Server IP that Access Point will use to query server.

Secondary Radius Server IP Enter the Secondary Radius Server IP that Access Point will use to query the server.

Authentication Port Enter the Radius Server Authentication Port number to use. Default is 1812.

Accounting Port Enter Radius server Accounting Port to use. Default is 1813.

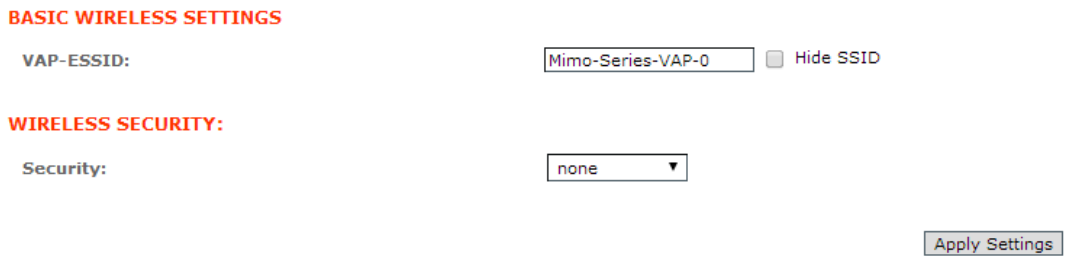
Radius Secret Key Enter Radius server Secret Key that Access Point to use to authenticate itself with radius server.

IEEE802.1x Key Rotation Enter time in seconds. Time before activate key rotation in authentication process for higher security.

IEEE802.1x Key Length This is the key length of the initial seed key. Select 64 or 128bit.

Virtual Access Point (VAP)

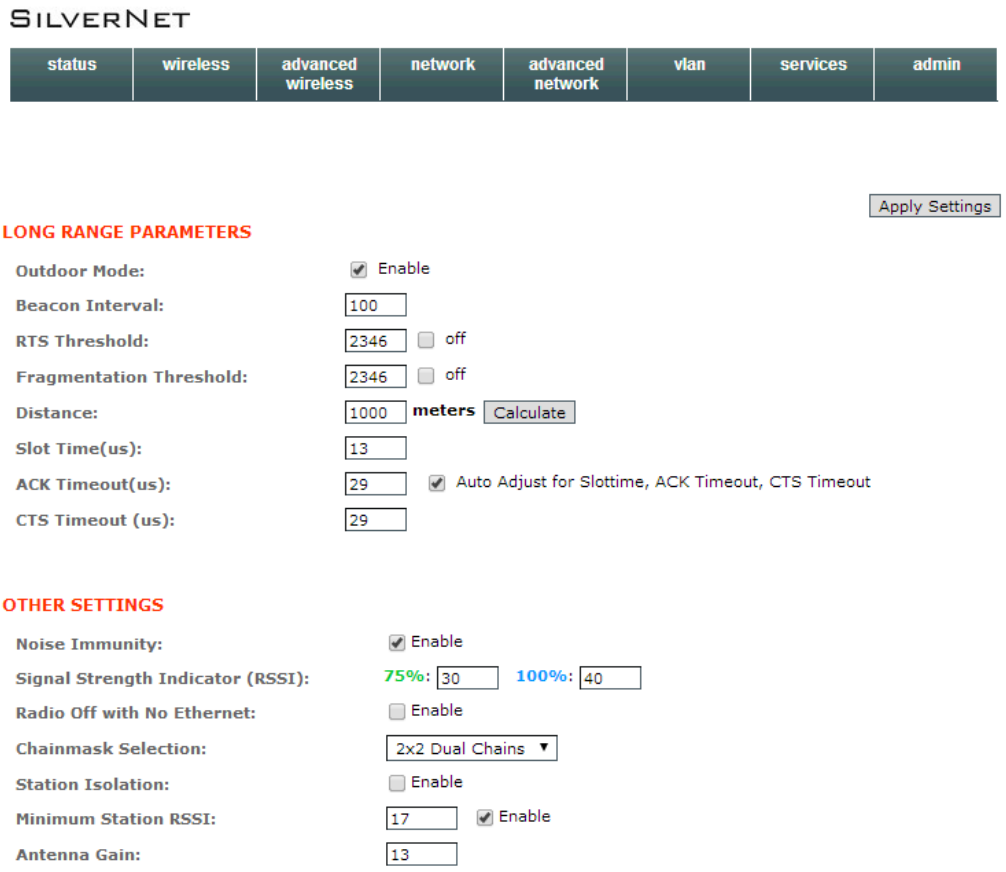
Virtual AP (VAP) implements mSSID (Multi-SSID) whereby a single wireless card can be setup with up to 3 virtual SSID connections. Each VAP can be set with different security authentication mode.



All VAPs are created from the same radio and they all share the same wireless channel, country code, channel spectrum width and transmit power.
Once settings have been applied, you will need to tick the enable button on the wireless page and apply settings.

Advanced Wireless Tab

The *Advanced Wireless* tab contains the long distance parameter settings and a few other advanced settings. Only technically advanced users who have Sufficient knowledge about WLAN technology should use the advanced wireless settings.



Apply Settings To apply any settings to the radio, click **Apply Settings** Once you have done this it will ask you to either Save or Discard any changes To immediately save your changes, click **Save**. To cancel your changes, click **Discard**.

Long Range Parameters

Outdoor Mode Check to enable outdoor mode
Beacon Interval This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router which carries the SSID, channel number and security protocols. We recommend using the **default setting of 100**.
In poor reception areas you may turn this down to 50.
RTS Threshold This value is set to **2346 as default**. We recommend leaving this setting. The device sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Fragmentation Threshold This is set to **2346 as default.** We recommend leaving this setting. This specifies the maximum size for a packet before data is fragmented into multiple packets.

If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting it too low may result in poor network performance. Only minor modifications of this value are recommended.

Distance To specify the distance value, manually enter the value and then click calculate. The values for Slot Time, ACK Timeout, CTS Timeout will be calculated automatically.

Other Settings

Noise Immunity Check to enable. When enabled, it automatically adjusts the signal/noise level for best performance. In a low noise environment it is recommended you turn off this function.
Signal Strength Indicator (RSSI) You can configure the LEDs on the device to light up when received signal levels reach the values defined in the two fields.

The default values are 75% (30) and 100% (40)
When the RSSI is greater than 30 the 75% LED will turn on.
When the RSSI is greater than 40, both the 75% and 100% LEDs will turn on.
For long distance installations when the signal strength is expected to be lower (at about 30-40), the values can be adjusted to compensate.
The LEDs values can be adjusted as follows:

- 75% (RSSI value=15)
- 100% (RSSI value=22)

Radio Off with No Ethernet When checked, the device will automatically stop any wireless broadcast if it **does not** detect any Ethernet connection.
Chainmask Selection Available selections are:

- **1x1 Left Chain** This will force the radio card to operate with 1 spatial stream on the left port of radio card only.
- **1x1 Right Chain** This will force the radio card to operate with 1 spatial stream on the right port of radio card only.
- **2x2 Dual Chain** This will enable the radio card to operate with 2 spatial streams on both of the radio card ports.

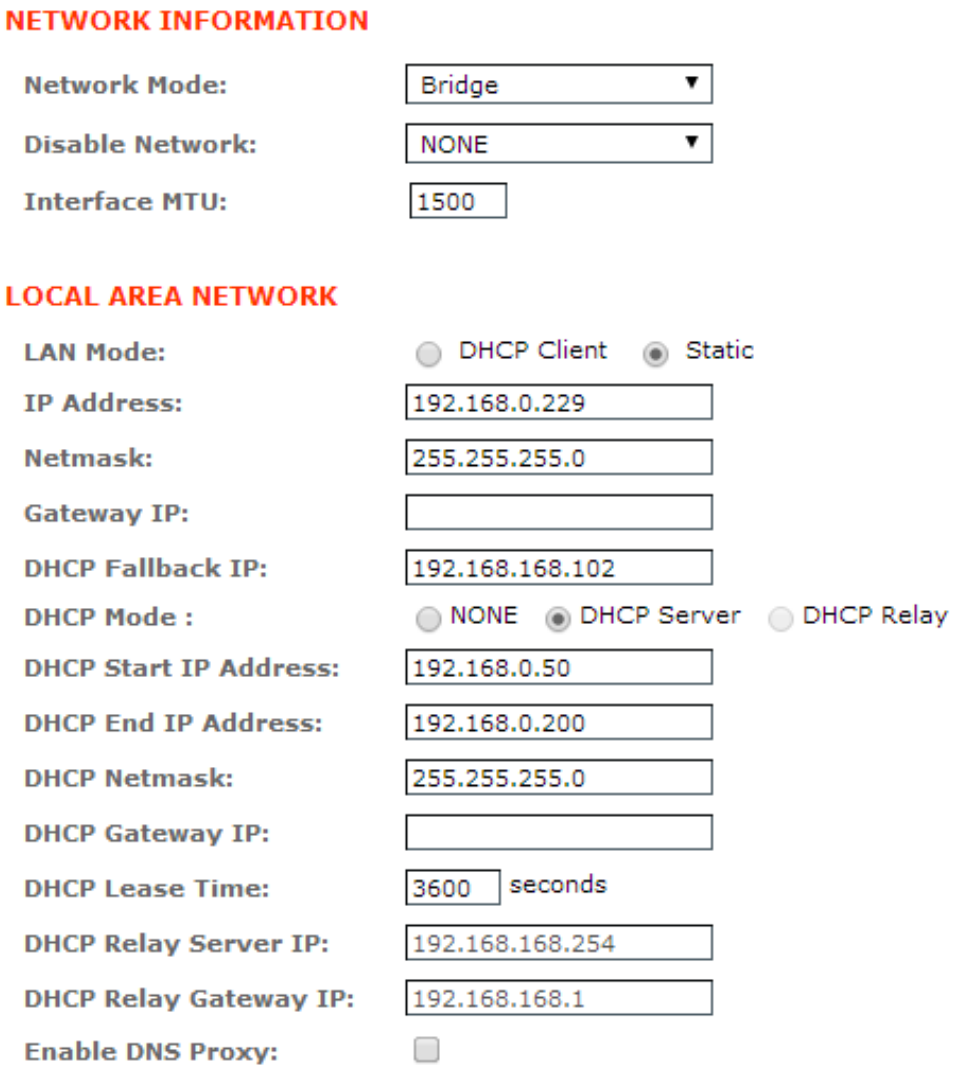
Multiple streams increase data transfer performance significantly.

Station Isolation When checked, it prevents any wireless stations/clients connected to the same AP from discovering each other.
Minimum Station RSSI When enabled, if the signal strength of any device connected to the AP falls below the value in this box, the AP will drop the connection.
Antenna Gain This should be set to match the antenna gain (in dBi) of the antenna you have connected to the wireless device.

For example, if you have a BASE 95 with an Omni antenna – set the gain to 12 (because it is a 12dBi Omni antenna). If you have a sector antenna then set the value as 16 (because it is a 16 dBi antenna).

Network Tab

The Network tab allows you to configure the IP address of the device as well as any DHCP settings and bandwidth control settings



Network Information

Network Mode Select between Bridge mode (default) and Router mode. Bridge mode is what you need to use for a point to point link.
Disable Network You can disable the LAN so that only the wireless part of the device is working. You will only be able to access the device via another wireless device that is connected to it.
Interface MTU By default, any Ethernet interface has its maximum transmission unit (MTU) size set to 1500 bytes, which is the maximum and expected value for Ethernet frames. If packets larger than 1500 bytes are expected on your network you can increase the MTU size

Local Area Network

LAN Mode Static Here you can enable **DHCP Client** or **Static** (default)

DHCP Client If enabled, your device will get an IP address automatically from the network. There must be a DHCP server on your network for this to work.
Static Allows you to enter a static IP address.

IP address Enter the IP address you wish to give to the device. You will use this IP address to access the device interface.
Netmask Enter the class for the IP address. The default is a class C value of 255.255.255.0
Gateway (optional) Enter the gateway IP address of the network the device is connected to.
DHCP Fallback IP Enter an IP address that the device should use if there is no DHCP server to give it an IP address.
DHCP Mode select none, DHCP server or DHCP relay.

None DHCP function disabled
DHCP Server Check to enable. The device will act as a DHCP server hand out IP addresses automatically.
DHCP Relay Check to enable. Enter the IP address of the remote DHCP server where the DHCP Client request will be relayed to.

DHCP Start IP Address Enter the starting IP address to be issued
DHCP End IP Address Enter the last IP address the server will issue.
DHCP Lease Time Enter the new lease time in seconds.
DHCP Server Relay IP Enter the IP address of the remote DHCP server where the DHCP Client request will be relay to get the IP address.
DHCP Gateway Relay IP Enter the IP address of the remote gateway where the DHCP Client request will be relay to get the gateway IP address.
Enable DNS Proxy If enabled the router operation will act as proxy to resolve all DNS requests.

DHCP Reservations

If you want a device to have a specified IP address, then enter the details here. Enter the IP address you want, the device MAC address and a small description. Click add once you are done.

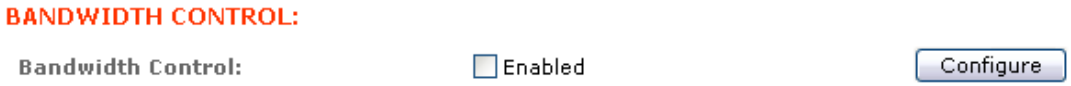
DHCP reservation is a process in which a particular IP address is mapped with one computer that is typically a server that needs to have a same IP address permanently. When this is done, every time the target DHCP client computer requests an IP address from the DHCP server, the mapped IP address is assigned to it. Since the IP address is reserved for a particular computer while specifying DHCP reservation, it is not assigned to any other computer even if it is the only address available in the DHCP address pool.

Domain Name Server Addresses

If you have specific DNS servers you like to use, you can type them in here.
If you want the device to obtain DNS server addresses automatically the please check the relevant option.

Primary DNS IP Enter the primary DNS IP address
Secondary DNS IP Enter the secondary DNS IP address

Bandwidth Control



To enable bandwidth control, please click configure.
Download Enter the download limit for the device
Upload Enter the upload limit of the device

An entry value of "0" means no bandwidth limit between the 2 interfaces.
An entry value of "2000" means 2000Kbit or 2Mbit bandwidth limit between the 2 interfaces.
The default is "0"

Router Mode

In Router Mode, the device also operates as a router.
Either the wireless or Ethernet can be setup as a WAN connection to a broadband modem. The Device supports several types of broadband connections such as Static IP, Dynamic IP and PPPoE. For setup details refer to the respective section.

Static IP Address Use Static IP Address if you have been given a fixed IP from your ISP.
Dynamic IP Address With Dynamic IP Address the device automatically requests an IP address from the modem or ISP.
PPP over Ethernet (PPPoE) choose this option to obtain an IP address, Gateway. IP and DNS address dynamically from the external PPPoE server.

Advanced Network Tab

The advanced network tab allows you to configure Router settings including NAT setup and firewall setups.

This tab will not open when in device is in Bridge mode.
To open the page, you must first enable Router mode on the Network page.

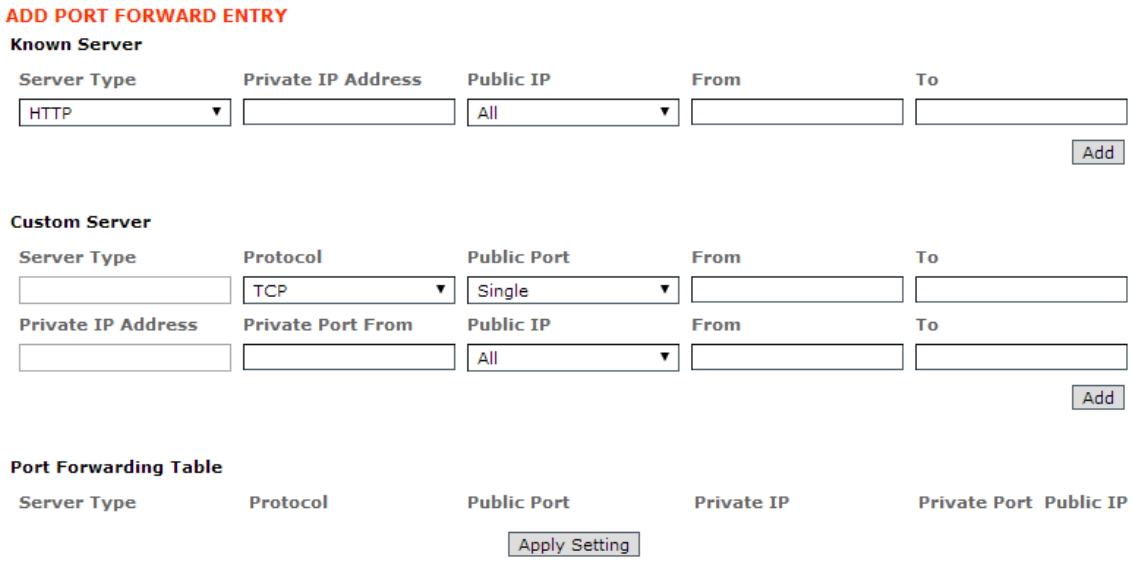
Nat Setup

NAT Network Address Translation (NAT) enables packets to be sent from the external network (WAN) to the local interface IP address and then sub-routed to other client devices on its local network while the PRO 95 device is operating in *Access Point* or *AP-Repeater* mode. Packets are routed in the reverse direction in *Station* mode.

DMZ DMZ (Demilitarized Zone) specifically allows one computer/device behind NAT to become "demilitarized", so all ports from the public network are forwarded to the ports of this private network, similar to a 1:1 NAT.

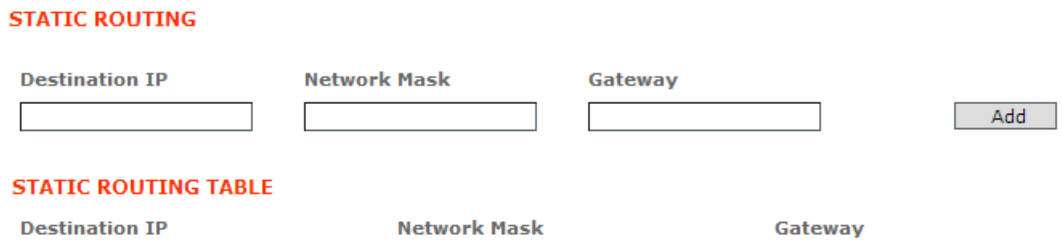
DMZ Private IP Specify the IP address of the local host network device. The DMZ host device will be completely exposed to the external network.

Port forwarding This allows specific ports on the local network to be forwarded to the external network (WAN). This is useful for a number of applications (such as FTP servers, VoIP, gaming) that require different host systems to be seen using a single common IP address/port.



Static Routing Table

You can manually add static routing rules to the system routing table; you can set a rule that a specific target IP address (or range of IP addresses) passes through a specific gateway.



Destination IP Specify the IP address of the destination.
Netmask Specify the Netmask of the destination.
Gateway IP Specify the IP address of the gateway.

Routing Information Protocol (RIP) Setup

RIPv1 is a classful routing protocol and it does not support VLSM (Variable Length Subnet Masking).
RIPv1 does not support authentication.
RIPv2 is classless routing and it supports VLSM (Variable Length Subnet Masking).
RIPv2 supports authentication.

Routing Info Protocol Check to enable RIP
Routing Info Protocol version Select from RIPv1 and RIPv2

Firewall Setup

Firewall

	On	Comment	Policy	IP Type	Source IP/Mask	Src Port	Destination IP/Mask	Des Port
1.			ACCEP	TCP				
2.			ACCEP	TCP				
3.			ACCEP	TCP				
4.			ACCEP	TCP				
5.			ACCEP	TCP				
6.			ACCEP	TCP				
7.			ACCEP	TCP				
8.			ACCEP	TCP				
9.			ACCEP	TCP				
10.			ACCEP	TCP				
11.			ACCEP	TCP				
12.			ACCEP	TCP				
13.			ACCEP	TCP				
14.			ACCEP	TCP				
15.			ACCEP	TCP				
16.			ACCEP	TCP				
17.			ACCEP	TCP				
18.			ACCEP	TCP				
19.			ACCEP	TCP				
20.			ACCEP	TCP				

Comment Enter a brief name for the service.
Policy Select Accept or Deny for the apply rule
IP Type Select ICMP, TCP, or UDP
Source IP/Mask enter the source IP address and Netmask
This is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets
Src Port Enter the source port number. This is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets.
Destination IP/Mask Enter the destination IP and Netmask is the Destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to.
Des Port Enter the destination port. This is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to

Multicast Routing Setup

Multicast Routing Enables multicast packet pass-through between local and external networks while the device is operating in *Router* mode. Multicast intercommunication is based on Internet Group Management Protocol (IGMP).

Remote Management Setup

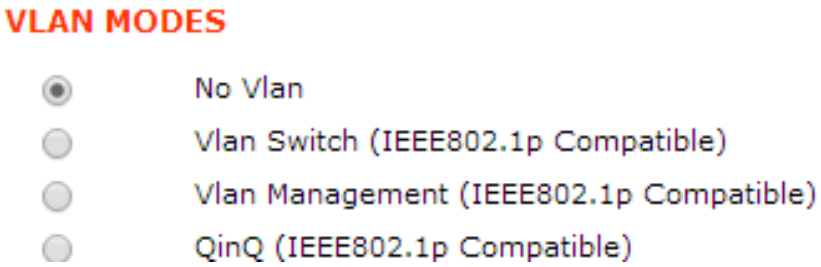
Remote HTTP/HTTPS Check box to enable
Remote HTTP port Set the port to use for remote management.

UPNP Setup

UPnP Allows the use of Universal Plug-and-Play (UPnP) for gaming, videos, chat, conferencing, and other applications.

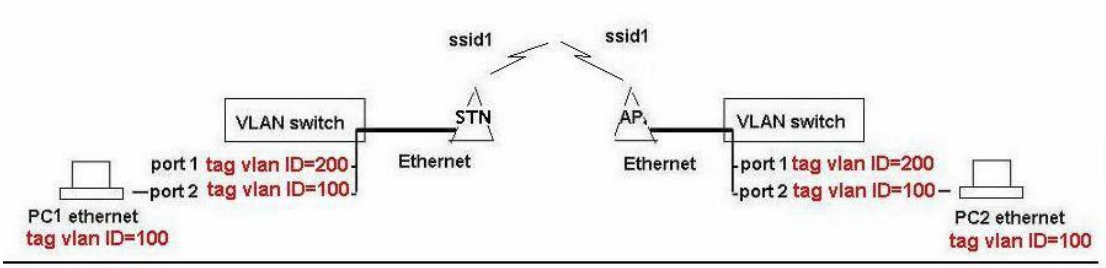
VLAN Tab

The *VLAN* tab allows you to create multiple Virtual Local Area Networks (VLANs). Only technically advanced users who have sufficient knowledge about WLAN technology should use the advanced wireless settings.

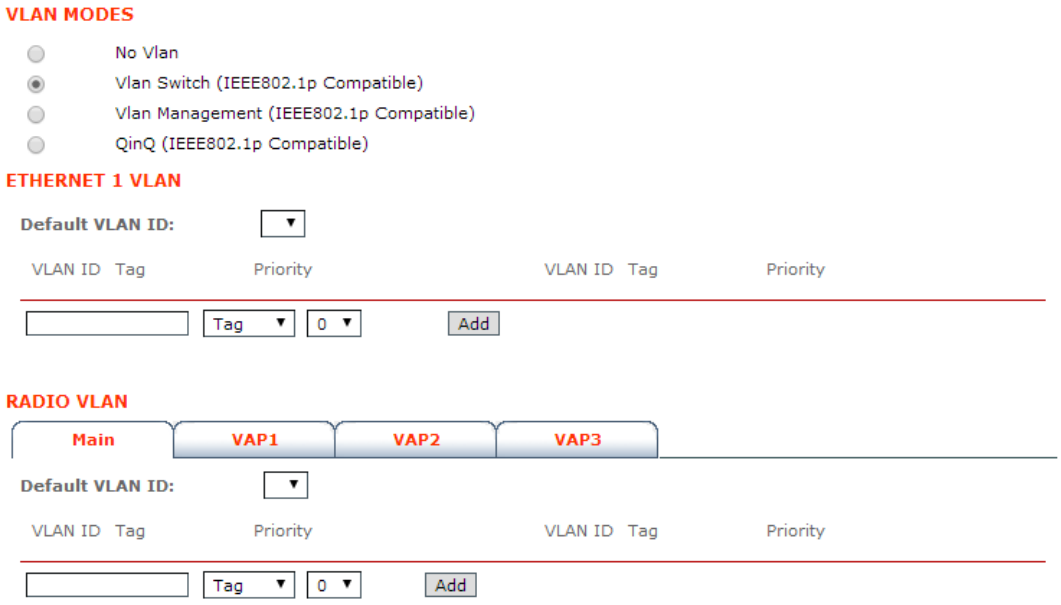


VLAN Modes

No VLAN The device will allow VLANS to pass through.



VLAN Switch Enables you to add VLAN tags to the Ethernet side and the wireless side of the device, including any Virtual Access Points you may have set up.



Ethernet VLAN

Tagged VLAN to add a tagged VLAN to the Ethernet port, type in the ID number, select **Tag** and click add.

Untagged VLAN to add an untagged VLAN to the Ethernet port, type in the ID number, select **Untag** and click add.

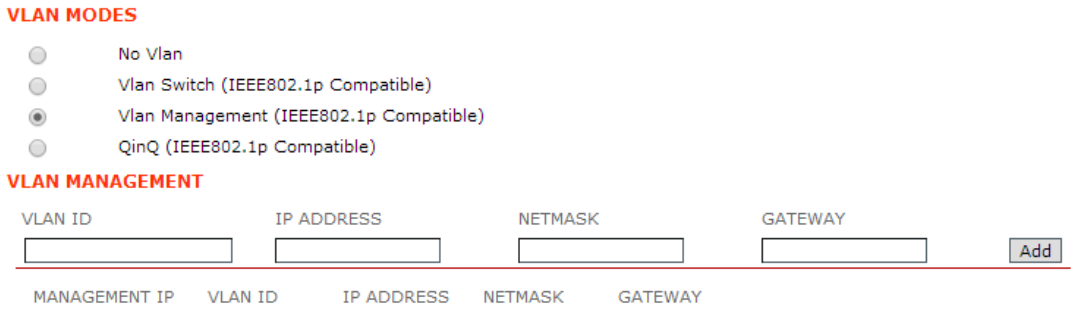
Radio VLAN

Tagged VLAN to add a tagged VLAN to the MAIN wireless SSID, type in the ID number, select **Tag** and click add.

Untagged VLAN to add an untagged VLAN to the MAIN wireless SSID, type in the ID number, select **Untag** and click add.

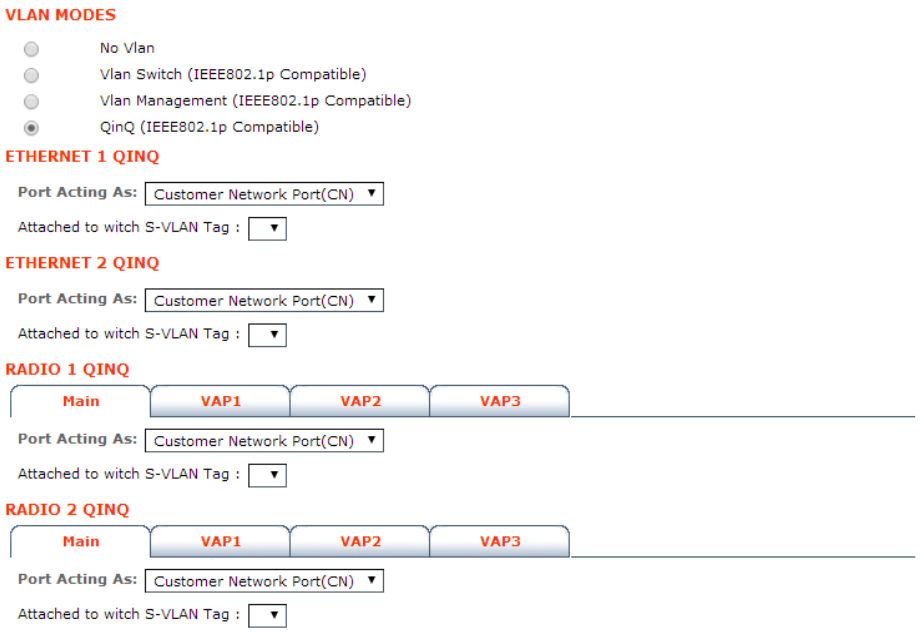
You can also set up any VLANS for any Virtual Access Points you may have created.

VLAN Management Enables you to control who can access the device by allowing only those on the same Tag VLAN ID to access the web page.



If you add a VLAN ID of 2001 and IP address of 192.168.0.20, then only computers on the same VLAN ID (2001) can open the web page using IP address 192.168.0.20

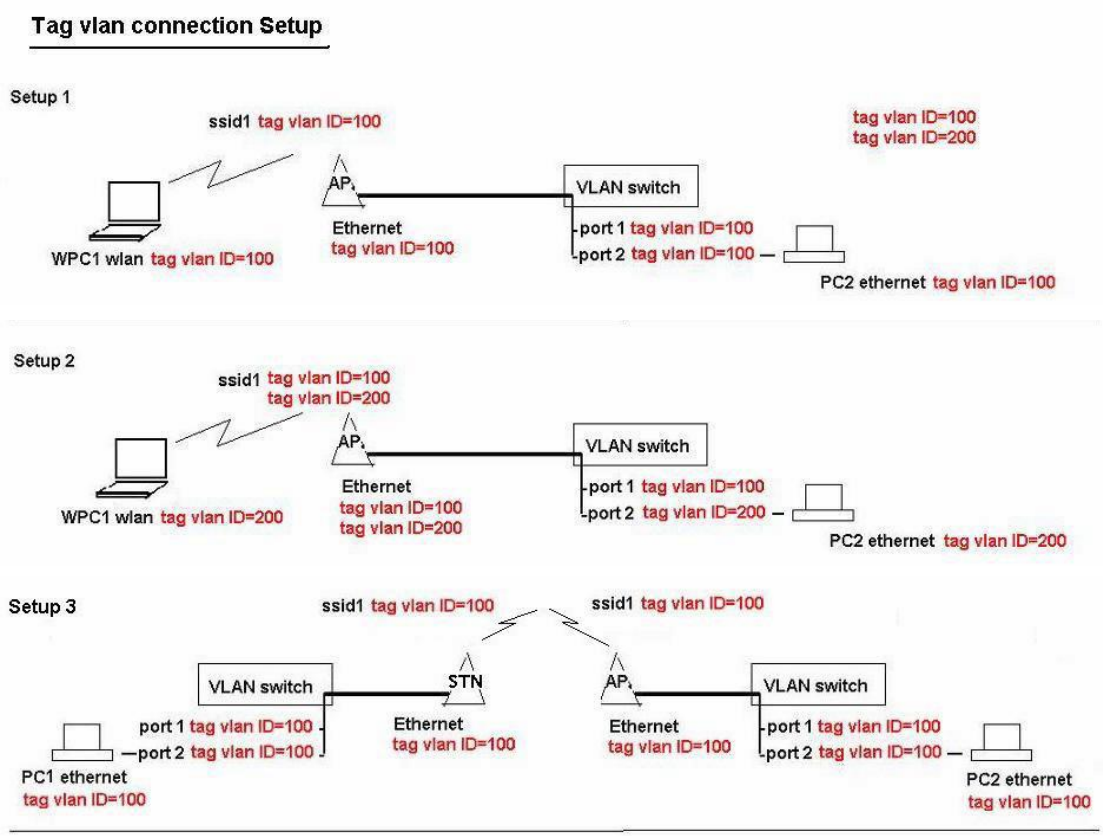
QinQ Can be used to achieve simple layer two VPN connectivity between sites by encapsulating one 802.1Q trunk inside another. Only use this if you are a very advanced user and have good knowledge of QinQ.



Provider Network Port (PN) Enter the VLAN ID of the Ethernet port or radio port and click add. You can also set the priority.
Customer Network port (CN) Select which VLAN tag to attach it to by selecting from the Dropbox.

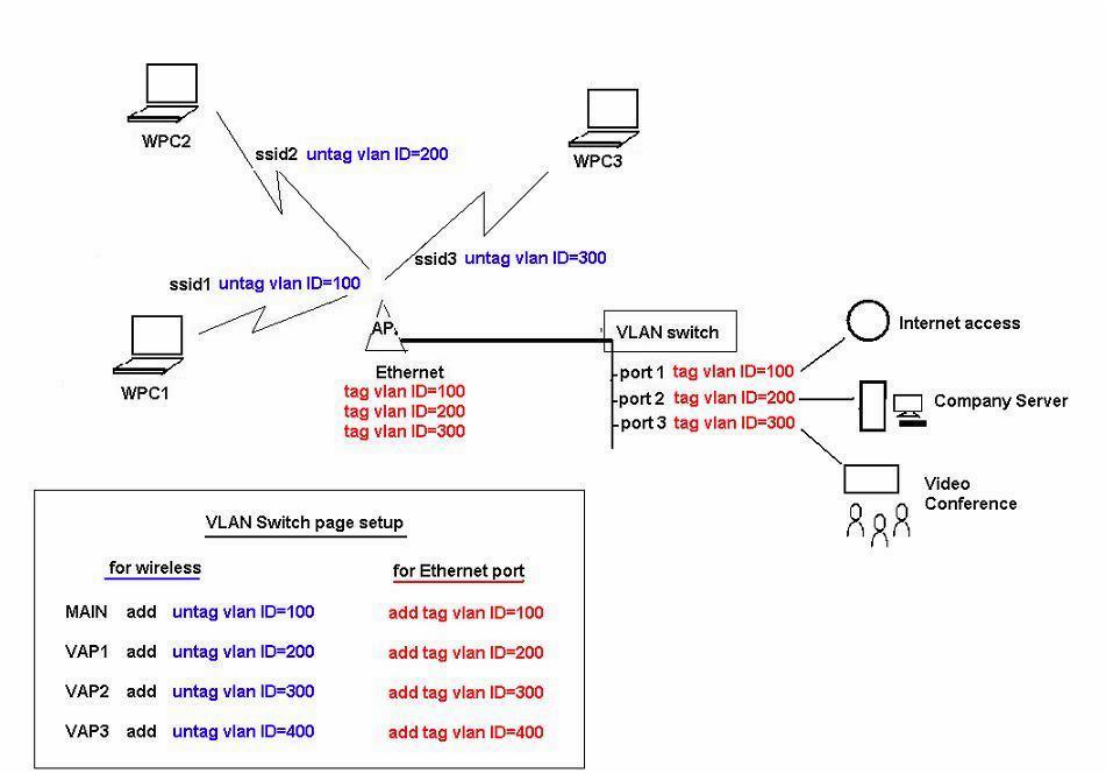
VLAN Examples

Tagged wireless VLAN to Tagged Ethernet VLAN setups



If you add a Tag VLAN to Ethernet side or Wireless side of the device you may lose connection to your PC if the Ethernet port or wireless card is not on the same Tag VLAN ID. If this happened, use the reset button to clear the config and re-configure.

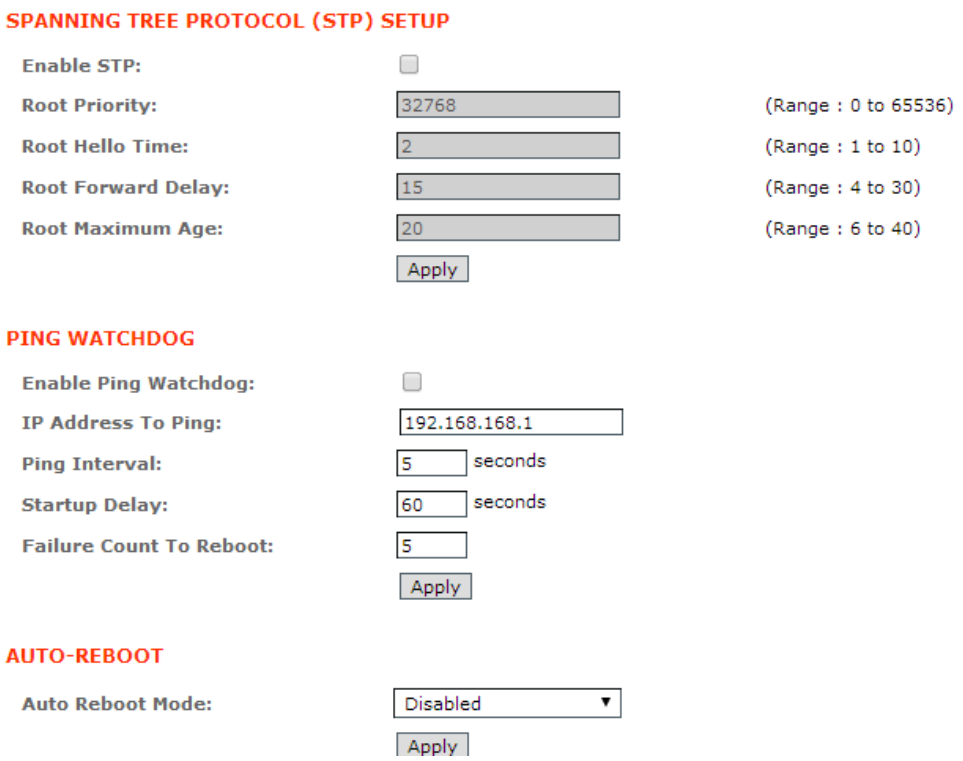
Untagged wireless VLAN to Tagged Ethernet VLAN setup



Multiple SSIDs with untagged VLAN connections connecting to a secure wired network with Tagged VLANs

Services Tab

The *Services* tab configures system management services like ping Watchdog, SNMP, servers (web, SSH, Telnet), NTP, DDNS, system log, and spanning tree.



Spanning Tree Protocol

Multiple interconnected bridges create larger networks using IEEE 802.1d Spanning Tree Protocol (STP), which is used for finding the shortest path within a network and eliminating loops from the topology.

Enable STP Check to enable Spanning Tree Protocol
Root Priority Enter the Root Priority. The default priority for switches is 32768
Root hello time The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec.
Root forward delay The forward delay is the time that is spent in the listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec.
Root maximum age The max age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information. This time is 20 sec by default, but you can tune the time to be between 6 and 40 sec.

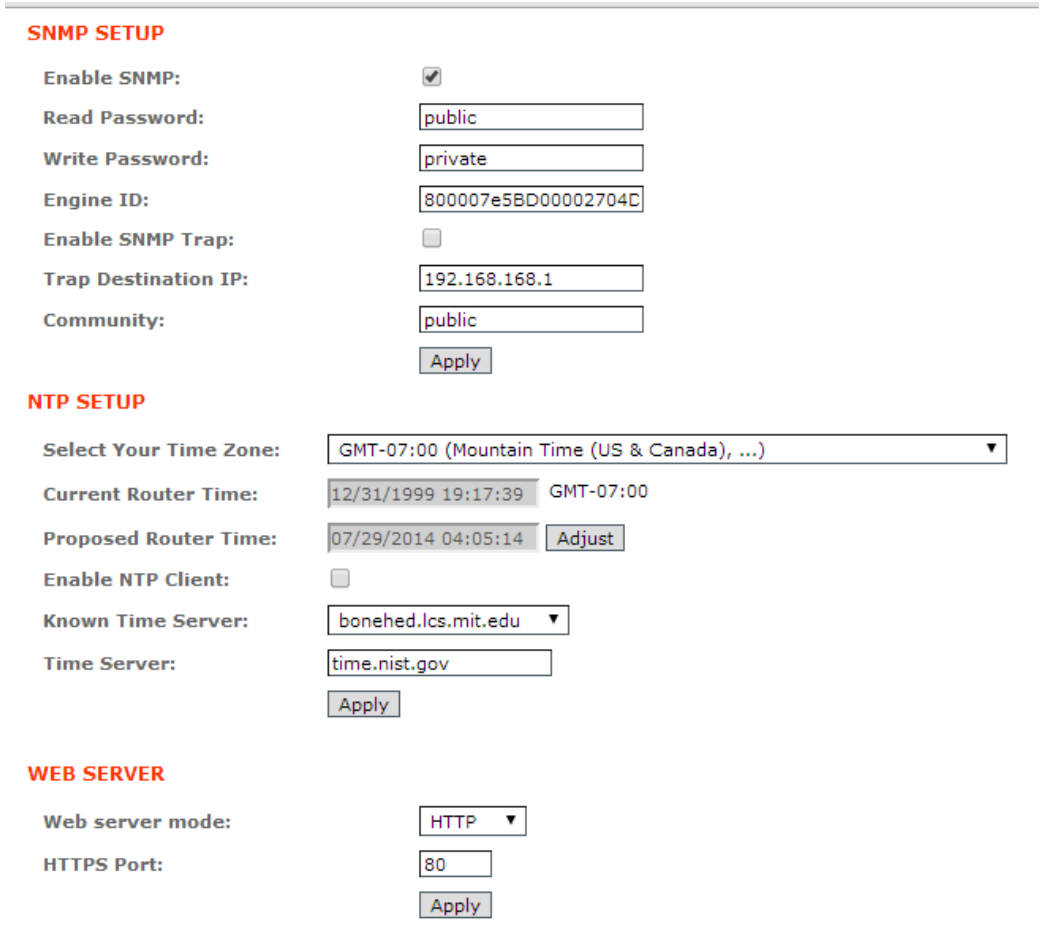
Ping Watchdog

Ping watchdog allows you to set an IP address that the device must monitor.
If the device fails to get a response from the IP address, Ping watchdog will reboot the device.

Enable Ping Watchdog Check this to enable ping watchdog.
IP address to Ping Specify the IP address of the target host to be monitored by Ping Watchdog.
Ping interval Specify the time interval (in seconds) between the ICMP echo requests that are sent by Ping Watchdog. The default value is *5* seconds. We recommend setting this to **10 seconds.**
Startup Delay Specify the initial time delay (in seconds) until the first ICMP echo requests are sent by Ping Watchdog. The default value is *60* seconds.
The Start up Delay value should be at least **60 seconds** as the network interface and wireless connection initialization takes a considerable amount of time if the device is rebooted.
Failure count to reboot Specify the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, Ping Watchdog will reboot the device. The default value is 5. We recommend **10 seconds**.

Auto Reboot

Auto reboot mode You can set to auto reboot the unit every X hours or at a certain time of the day.



SNMP Setup

Simple Network Monitor Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices.

Enable SNMP Check to enable SNMP
Read Password Enter the password for read only accounts
Write password Enter the password for administrator accounts. These are able to read and write.
Engine ID The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMP v3 messages.
If you do not specify an engine ID, one is generated when you enable the standalone SNMP agent.
Enable SNMP Trap Check to enable SNMP Trap
Trap Destination IP Enter the IP address to send the information when the trap is triggered.
Community Specify the SNMP community string. It is required to authenticate access to Management Information Base (MIB) objects and functions as an embedded password. The default SNMP Community is *public*.

NTP Setup

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. You can use it to set the system time on the device.

Select Your time Zone Select the correct time zone from the drop down menu
Current Router Time The current time on the router
Proposed Router Time The proposed time on the router
Enable NTP Client Check to enable NTP
Known Time Server You can select a time server from the drop down list
Time Server Enter your preferred time server. Default is time.nist.gov

WEB Server

Web Server Mode By default, HTTP service is enabled. You can set to HTTPS.
HTTPS Port If HTTP mode is used, specify the TCP/IP port of the web server. The default is *80*. If secure HTTPS mode is used, specify the TCP/IP port of the web server. The default is *443*.

Telnet Server

Enable Telnet Server Check to enable.
Server Port Specify the TCP/IP port of the Telnet server.

SSH Server

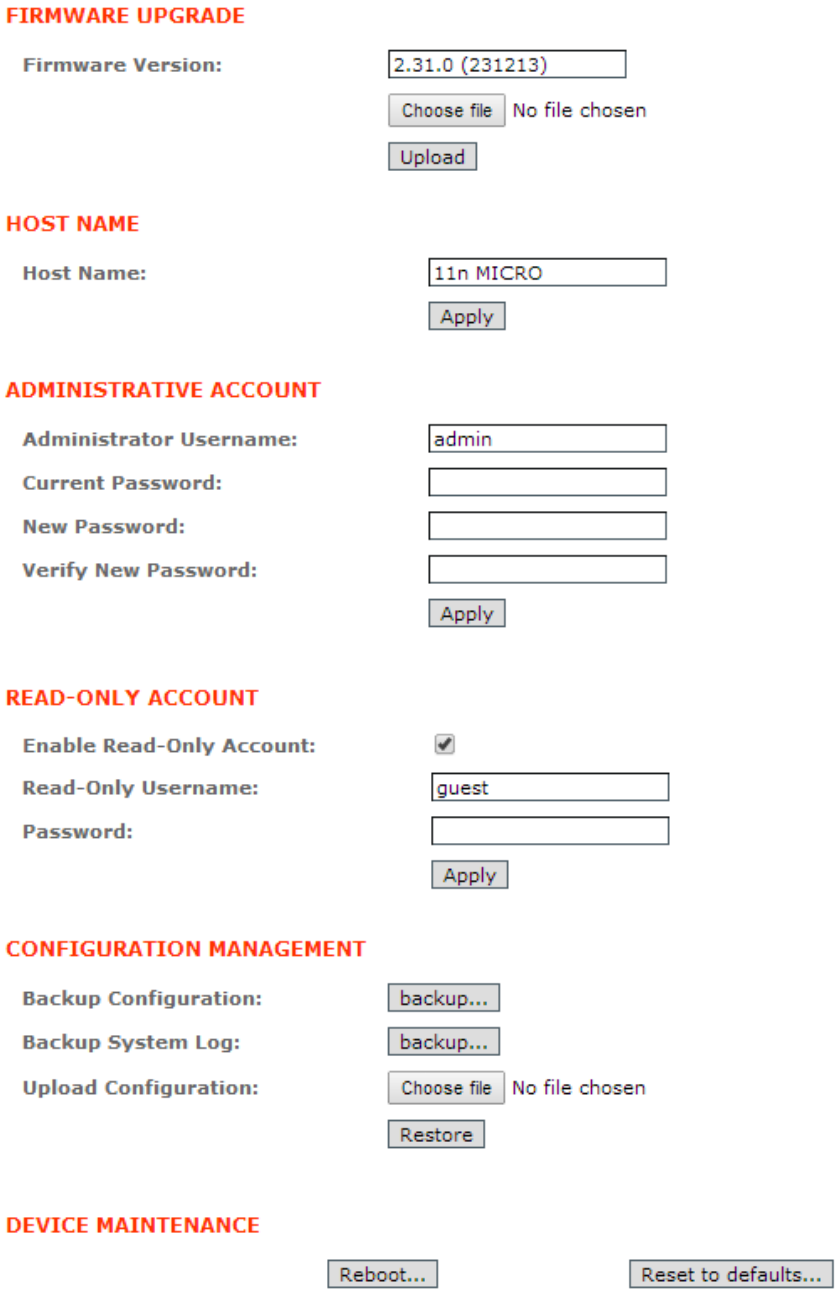
Enable SSH Server Check to enable.
Server Port Specify the TCP/IP port of the SSH server.

System log

Enable System Log Check to enable.
Logging IP/Domain name Enter the IP address or domain name of the host that receives syslog messages. Properly configure the remote host to receive syslog protocol messages.
Logging Port The TCP/IP port that receives syslog messages. *514* is the default port for the commonly used system message logging utilities.

Admin Tab

The *Admin* tab contains administrative options. This page enables the administrator to reboot the device, reset it to factory defaults, upload new firmware, back up or upload the configuration, and configure the administrator account.



Firmware Upgrade

Firmware Version Displays the current firmware
Choose File Select the firmware file you wish to upgrade.
Upload Click upload to begin the update process.

Please be patient, as the firmware upgrade routine can take 3-7 minutes. The device will be un-accessible until the firmware upgrade is completed. Do not switch off the device! Do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!

Host Name

Host Name Enter a name for your device

Administrative Account

Administrator Username Enter an admin username. Default is admin
Current Password Enter your current password. Default is password
New Password Enter a new password
Verify New Password Re-enter your new password

Read Only Account

Enable Read Only Account Check to enable.
Read Only Username Enter a read only username. Default is guest
Password Enter a password. No password is set by default.

Configuration Management

Backup Configuration Click to save down the configuration file of the device.
Backup System Log Click to save down the system log of the device.
Upload Configuration Select the configuration file you wish to upload and click the restore button.

Device Maintenance

Reboot This reboots the device
Reset to defaults This will reset the device to the default factory settings (IP address 192.168.168.1)

Contact Us

SilverNet Ltd

2 Vermont Place
Tongwell
Milton Keynes
MK15 8JA

Online Resources

If you need any further assistance go to our website download centre:
www.silvernet.com/downloadcentre/

Read the easy as 1-2-3 setup guide
http://www.silvernet.com/assets/Easy_as123_guide_1.pdf

View our troubleshooting guide:
http://www.silvernet.com/support/frequently-asked-questions/

Use our online ticket support:
www.silvernet.com/support/

Email us at support@silvernet.com

Call our support team on 08712233067

www.silvernet.com