

# SILVERNET

WIRELESS-NETWORK-SOLUTIONS

## PRO RANGE



PICO



MICRO



LITE



MAX

User Manual

## TABLE OF CONTENTS

Introduction .....	4
Supported Products .....	4
Wireless Modes .....	4
System Requirements .....	4
Packing list .....	5
The Enclosure and LED indicators .....	6
Configuration .....	7
Getting Started .....	7
Navigation .....	8
Status .....	9
Overview .....	10
Realtime Graphs .....	12
Admin Tab .....	13
System .....	13
Administration .....	15
SNMP .....	16
LED Configuration .....	18
Backup/Flash Firmware .....	19
Reboot .....	19
Services .....	21
Dynamic DNS .....	21
Network Tab .....	27
LAN Interface .....	28
DHCP Server .....	29
Wireless Interface .....	32

Device Configuration ..... 33

Interface Configuration..... 37

Wireless Security..... 39

VLANS ..... 42

Diagnostics..... 44

Standards..... 45

    Declaration of Conformity ..... 45

Warnings..... 46

    Radio frequency Interference Requirements..... 46

Troubleshooting..... 48

Warranty..... 48

Contact SilverNet ..... 48

Copyright Information ..... 48

Other SilverNet Products ..... 49

    Pro Range..... 49

    Industrial Network Transmission ..... 49

    Intelligent Wi-Fi Solutions ..... 49

    Industry Leading Technical Support..... 49

## INTRODUCTION

This User Guide describes the firmware version 2.1.3 and above which is integrated into all Pro Range products provided by SilverNet Ltd.

## SUPPORTED PRODUCTS

This manual covers all GEN4 products listed below:

- PICO
- MICRO
- LITE
- MAX

For more information, visit [www.silvernet.com](http://www.silvernet.com)

## WIRELESS MODES

The Pro Range supports the following wireless modes:

- Station
- Station WDS
- Access Point
- Access Point WDS

## SYSTEM REQUIREMENTS

- Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, or Mac OS X
- Web Browser: Mozilla Firefox, Apple Safari, Google Chrome, or Microsoft Internet Explorer 9 (or above)

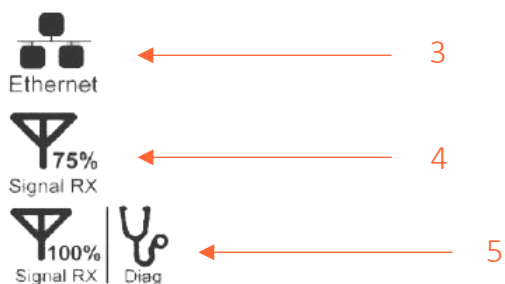
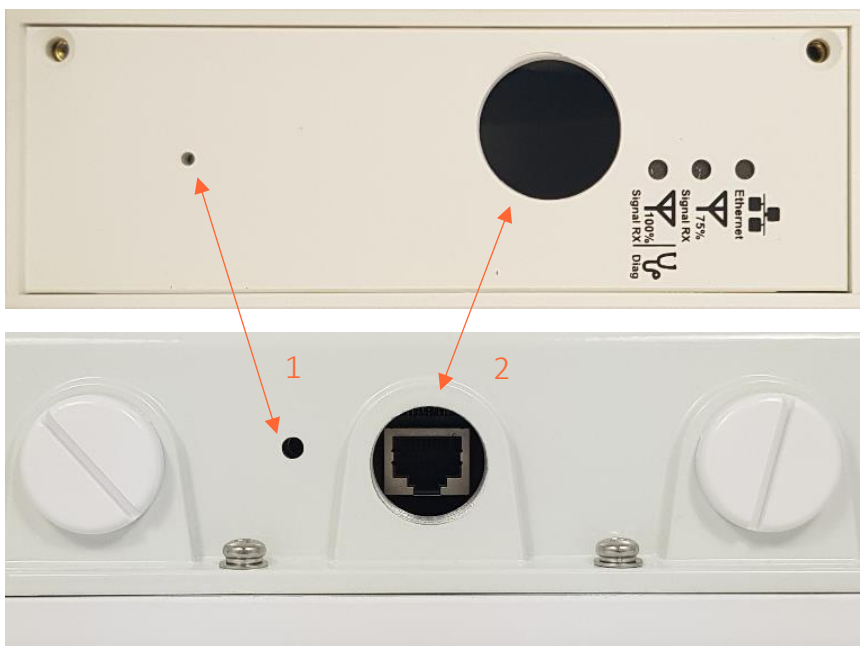
## PACKING LIST

Please check the following items in the package before installing the device

Wireless Radio	1 piece
User manual	1 copy
Cable Gland	1 piece
Mounting bracket	1 piece
Power over Ethernet Injector	1 piece
Power cable	1 piece
Set of screws	1 piece

Please contact your distributor immediately for any missing or damaged items.

## THE ENCLOSURE AND LED INDICATORS



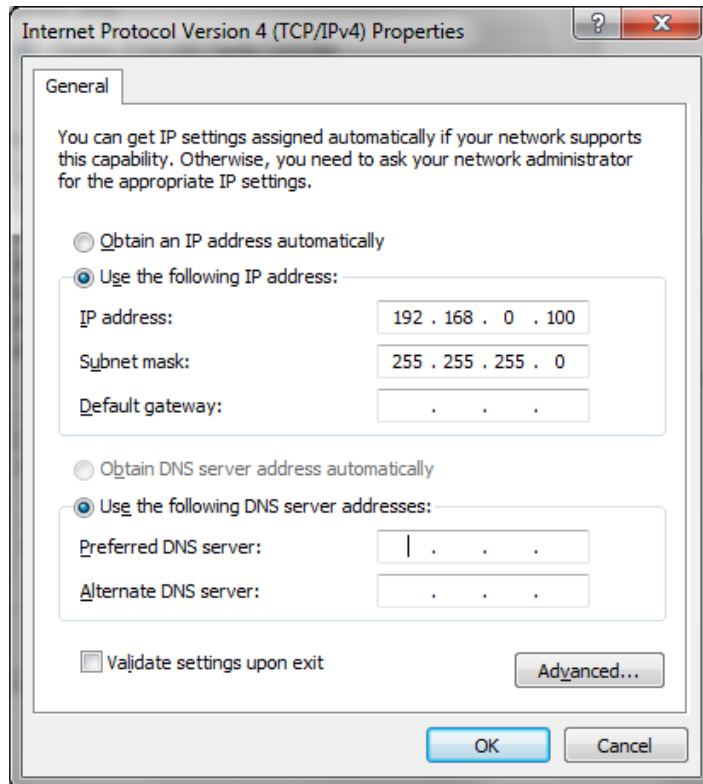
Mark	Name	Function
1	Reset Button	Press to reboot the device manually Hold to rest the device to factory settings
2	Ethernet Port (PoE)	10/100Mbps Ethernet port and PoE power input (48V DC)
3	Ethernet link LED	“On/Blinking”: Power is being supplied and a link has been established to the network. “Off”: No power and/or the Ethernet port has no connection
4	75% Signal Rx LED	“On”: Signal Strength is at 75% “Off”: Signal Strength not at 75%
5	100% Signal Rx LED	“On”: Signal Strength is at 100% “Off”: Signal Strength not at 100% “Blinking”: Device is in diagnostic mode

## CONFIGURATION

### GETTING STARTED

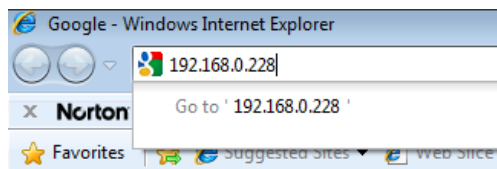
To access the Pro Range Configuration Interface, perform the following steps:

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.

Pro Range products are pre-configured to IP address 192.168.0.229/192.168.0.228



**If the unit has been reset, it will go to the default IP address of 192.168.1.1. You will need to change your Ethernet adapter IP address to 192.168.1.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 four main tabs, each with sub tabs which provide a web-based management page to configure a specific aspect of the SilverNet device:

**Status**   Admin   Services   Network   Logout

- **Status** The “**Status Tab**” displays device status, system logs, and real-time graphs.
- **Admin** The “**Admin Tab**” displays basic system properties, NTP configuration, administration, SNMP configuration, LED Configuration, file and firmware management and Reboot.
- **Services** The “**Services Tab**” allows you to configure Dynamic DNS.
- **Network** The “**Network Tab**” configures the network operating mode; This includes LAN Interface settings, Wireless Settings, VLAN Management and Network Diagnostics.
- **Logout** The “**Logout Tab**” allows you to logout of the unit.

**Apply Settings** To apply any settings to the radio, click **Save and Apply**



## STATUS

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.

### AP status page

### Station status page

When using the alignment buzzer, the faster the beeps the better the signal quality.

## OVERVIEW

**Wireless** This shows you the SSID, operating mode, channel frequency, bitrate, BSSID, encryption mode and the DFS status.

**Associated Stations** Displays the MAC address, SSID and signal information of any stations connected to the AP.

**System** Displays the name of the device, the firmware version and the current system date and time. The date and time are displayed in DAY-MONTH-YEAR HOURS:MINUTES:SECONDS format.

**Memory** Displays the total amount of memory on the board and shows how much is free in kB (Kilobytes).

**Network** Displays local device information including the current uptime, MAC address and IP address.

## Wireless Parameters

**SSID** Displays the name of the wireless network that the AP is transmitting, the Service Set Identifier (SSID), is what you will see if you scan with your laptop.

**Mode** This is “Master” if the device is set in AP mode or AP WDS Mode.

This will show as “client” if the device is in station mode or station WDS mode.

**Channel** Shows the channel number and frequency that the device is using.

**Bitrate** This is the maximum bitrate supported by the radio.

**BSSID** Displays the MAC address of the device.

**Encryption** Displays the wireless encryption used.

**DFS Status** If DFS is enabled, the device will automatically switch channels if any radar is detected on the current channel it is using

### Associated Stations Parameters

**MAC Address** Displays the MAC address of the device.

**Network** States the name of the wireless network.

**Noise** Displays the received noise power at the AP.

**RSSI** Displays the received signal strength.

**TX Rate** shows the transmit bitrate of the device.

**RX Rate** shows the receive bitrate of the device.

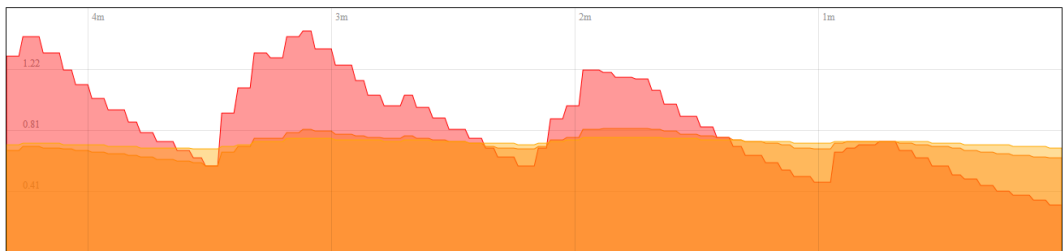
**TX CCQ** Displays the transmission quality in %. A higher percentage means better wireless connection quality.

**Up Time** Displays the current uptime of the paired device.

## REALTIME GRAPHS

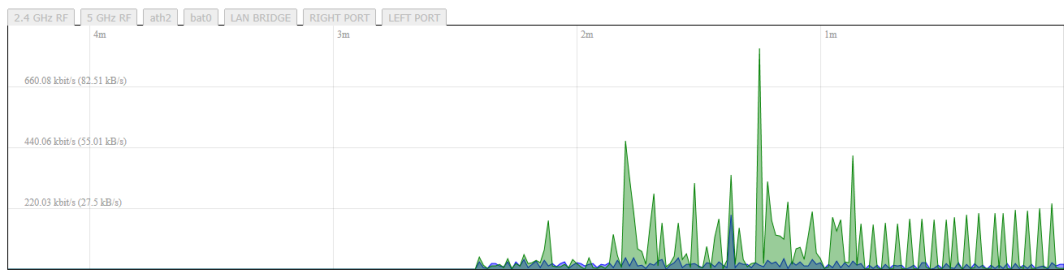
There are four different graphs, you can view Load, Traffic, Wireless and connection graphs.

### Realtime Load



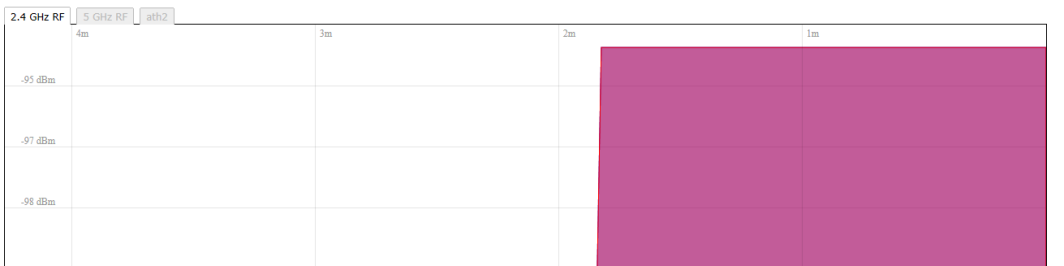
<b>1 Minute Load:</b> 0.32	<b>Average:</b> 0.32	<b>Peak:</b> 1.48
<b>5 Minute Load:</b> 0.63	<b>Average:</b> 0.63	<b>Peak:</b> 0.83
<b>15 Minute Load:</b> 0.70	<b>Average:</b> 0.70	<b>Peak:</b> 0.77

### Realtime Traffic



<b>Inbound:</b> 20.45 kbit/s (2.56 kB/s)	<b>Average:</b> 17.17 kbit/s (2.15 kB/s)	<b>Peak:</b> 199.09 kbit/s (24.89 kB/s)
<b>Outbound:</b> 3.95 kbit/s (0.49 kB/s)	<b>Average:</b> 38.69 kbit/s (4.84 kB/s)	<b>Peak:</b> 800.1 kbit/s (100.01 kB/s)

### Realtime Wireless

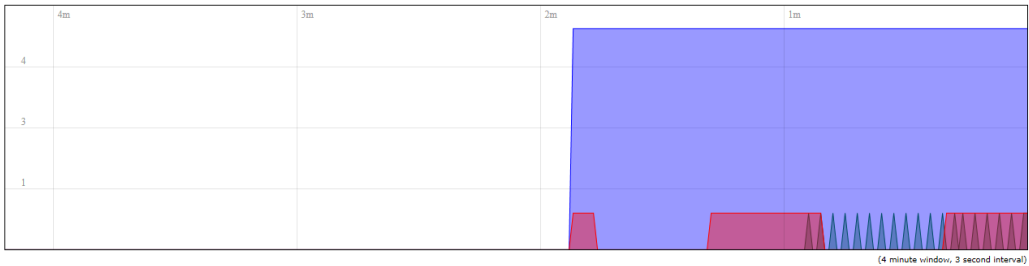


<b>Signal:</b> -95 dBm (SNR 0 dBm)	<b>Average:</b> -95 dBm (SNR 0 dBm)	<b>Peak:</b> -95 dBm (SNR 0 dBm)
<b>Noise:</b> -95 dBm	<b>Average:</b> -95 dBm	<b>Peak:</b> -95 dBm

### Realtime Connections

This page gives an overview over currently active network connections.

#### Active Connections



<b>UDP:</b> 6	<b>Average:</b> 6	<b>Peak:</b> 6
<b>TCP:</b> 1	<b>Average:</b> 0	<b>Peak:</b> 1
<b>Other:</b> 1	<b>Average:</b> 0	<b>Peak:</b> 1

## ADMIN TAB

The Admin tab contains administrative options. This page enables the administrator to configure System Properties, Time Synchronisation, Logging Settings, User Management, Web Administration, SNMP Configuration, LED Configuration, Backup config files / flash new firmware and reboot the device.

## SYSTEM

**SILVERNET** MICRO | v2.1.3(170821) | Auto Refresh: on Changes: 0

Status **Admin** Services Network Logout

**System** Administration SNMP LED Configuration Backup / Flash Firmware Reboot

### System

Here you can configure the basic aspects of your device like its hostname or the timezone.

#### System Properties

General Settings **Logging**

Local Time	Tue Aug 17 10:14:28 2021 <input checked="" type="checkbox"/> Sync with browser
Hostname	MICRO <input type="text"/>
Timezone	UTC <input type="text"/>

#### Time Synchronisation

Enable NTP client	<input checked="" type="checkbox"/>
Provide NTP server	<input type="checkbox"/>
NTP server candidates	<input type="text" value="0.pool.ntp.org"/> <input type="text" value="1.pool.ntp.org"/> <input type="text" value="2.pool.ntp.org"/> <input type="text" value="3.pool.ntp.org"/>

## General Settings

**Local Time** Displays the local time according to the time zone.

**Host Name** Enter a name for your device.

**Time Zone** Select the correct time zone from the drop-down menu.

**Sync with browser** Click to sync device time with your browsers.

## Time Synchronisation

**Enable NTP Client** Check to enable NTP.

**Provide NTP Server** Enter your preferred NTP Server under NTP candidates.

**NTP Server Candidates** These are the sources where you get your time information. We recommend you enter at least three for accurate time synchronisation.

## System

Here you can configure the basic aspects of your device like its hostname or the timezone.

### System Properties

General Settings	Logging
System log buffer size	64 <input type="text"/> <input type="button" value="kB"/>
External system log server	0.0.0.0 <input type="text"/>
External system log server port	514 <input type="text"/>
Log output level	Debug <input type="button" value="v"/>
Cron Log Level	Normal <input type="button" value="v"/>

### Time Synchronisation

Enable NTP client	<input checked="" type="checkbox"/>
Provide NTP server	<input type="checkbox"/>
NTP server candidates	<input type="text" value="0.pool.ntp.org"/> <input type="button" value="x"/> <input type="text" value="1.pool.ntp.org"/> <input type="button" value="x"/> <input type="text" value="2.pool.ntp.org"/> <input type="button" value="x"/> <input type="text" value="3.pool.ntp.org"/> <input type="button" value="x"/>

## Logging

**System Log Buffer Size** Change the size of the log buffer.

**External System Log Server** Input an address that the system log is sent to.

**External System Log Server Port** Input an external server port.

**Log Output Level** Change the type of log report.

**Cron Log Level** Change the level of log report.

## ADMINISTRATION

Use this section to change the administrator password.

### Router Password

**SILVERNET** MICRO | v2.1.3(170821) Changes: 0

Status **Admin** Services Network Logout

System **Administration** SNMP LED Configuration Backup / Flash Firmware Reboot

#### Radio Password

Changes the administrator password for accessing the device

Password	<input type="password"/>
Confirmation	<input type="password"/>

**Password** Enter a new password.

**Confirmation** Re-enter your new password.

## SNMP

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices on an IP network.

**SILVERNET** MICRO | v2.1.3(170821) Changes: 0

Status **Admin** Services Network Logout  
System Administration **SNMP** LED Configuration Backup / Flash Firmware Reboot

### SNMP

Here you can configure your SNMP V2c and SNMP V3, read and write password

**SNMP Information**

Information	
SNMP Enterprise ID	44828
Contact	http://www.silvernet.com
Location	office

**SNMP Configuration**

General Settings <input type="checkbox"/> Trap <input type="checkbox"/>	
Enable SNMP	<input checked="" type="checkbox"/>
SNMP V2c Read Password	public
SNMP V2c Write Password	private
SNMP V3 Username	admin
SNMP V3 Auth Algorithm	MDS
SNMP V3 Auth Password	*****
SNMP V3 Privacy Algorithm	DES
SNMP V3 Privacy Password	*****

### SNMP Information

These identifiers are arbitrary and do not affect the server's function, but they are useful to have. The contact is the person who manages the server. The location is the server's physical location. Each of these parameters can be up to 64 characters.

**SNMP Enterprise ID** Enter the ID of the SNMP Server.

**Contact** Enter the name of the person who manages the server.

**Location** Enter the server's physical location.



## SNMP Configuration

### Enable SNMP Enable SNMP

**SNMP V2c Read Password** Sets the community string for read-only access (to the variables on the SNMP agent) by the Network Management Station (NMS). The NMS is the software that runs on the SNMP manager. (default: public)

**SNMP V2c Write Password** Sets the community string for read-write access by the SNMP manager. (default: private) A community string identifies a group of SNMP agents. It is sent in clear text. It should be changed from the default string “public” or “private”. The variables on the SNMP agent can be classified into read-only or read-write variables.

**SNMP V3 Username** Sets the username for authentication. (default: admin)

**SNMP V3 Auth Algorithm** Shows the authentication algorithm used e.g. MD5.

**SNMP V3 Auth Password** Configures the password for user authentication. (default: password)

**SNMP V3 Privacy Algorithm** Shows the data encryption algorithm used e.g. DES.

**SNMP V3 Privacy Password** Sets the password for data encryption. (default: password)

#### SNMP Configuration

SNMP Configuration	
General Settings	Trap
Enable SNMP Trap	<input type="checkbox"/>
SNMP Trap IP Address	<input type="text" value="192.168.1.10"/>
SNMP Trap Port	<input type="text" value="162"/>

## SNMP Trap

**Enable SNMP Trap** Allows the SNMP agent to notify the SNMP manager of events.

**SNMP Trap IP Address** Sets the IP address of the SNMP manager which receives the trap messages.

**SNMP Trap Port** Sets the port number.

## LED CONFIGURATION

You can configure the LEDs on the device to light up when received signal levels reach the values defined in the four fields.

**SILVERNET** MICRO | v2.1.3(170821) Changes: 0

Status **Admin** Services Network Logout  
System Administration SNMP **LED Configuration** Backup / Flash Firmware Reboot

### LED Configuration

Customizes the behaviour of the device LEDs.

**Signal strength indicator interface**

Wireless interface

**Signal strength indicator LEDs**

LED 1 Flash	<input type="text" value="10"/>
LED 1 Solid	<input type="text" value="20"/>
LED 2 Flash	<input type="text" value="30"/>
LED 2 Solid	<input type="text" value="40"/>

**Signal Strength Indicator Interface** Choose the wireless interface (wireless network name) to display LEDs for.

**Signal Strength Indicator LEDs** Sets the received signal strength thresholds (in dBm), if the signal is above the threshold, the LED will light up.

## BACKUP/FLASH FIRMWARE

**SILVERNET** Changes: 0  
MICRO | v2.1.3(170821)

Status **Admin** Services Network Logout  
System Administration SNMP LED Configuration **Backup / Flash Firmware** Reboot

### Flash operations

**Backup / Restore**  
Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset".

Download backup:

Reset to defaults:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:  No file chosen

**Add Functionality**  
A key file can be uploaded here to add product features.

Key File:  No file chosen

**Flash new firmware image**  
Upload a compatible image here to replace the firmware running on this unit. Check "Keep settings" to retain the current configuration.

Keep settings:

Image:  No file chosen

### Backup / Restore

**Download Backup** Click to save down the configuration file of the device.

**Reset to Defaults** This will reset the device to the default factory settings (IP address 192.168.1.1)

**Restore Backup** Select the configuration file you wish to upload and click the restore button.

### Add Functionality

**Key File:** Select the Key file you wish to upload to add extra functionality to the device.

### Flash new firmware

**Keep Settings** Enable to keep the current settings after firmware upgrade.

**Choose File** Select the firmware file you wish to upgrade and click upload to begin the update process.

**Please be patient, as the firmware upgrade routine can take 5-10 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!**

### REBOOT

## System

### Reboot

Reboots the operating system of your device

[Perform reboot](#)

**Perform Reboot** This option will perform a reboot of your device.

## SERVICES

The Services tab provides useful and enhanced functions to help assist device operations.

### DYNAMIC DNS

Dynamic DNS (DDNS) allows the device to be reached from the internet via a URL by translating a URL like www.silvernet.com to an IP address like 206.190.36.45

**SILVERNET** MICRO | v2.1.3(170821) | Auto Refresh: **on** Changes: 0

Status Admin **Services** Network Logout

**Dynamic DNS**

[Dynamic DNS](#)

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

**Hints**

[Show more](#) Follow this link  
You will find more hints to optimize your system to run DDNS scripts with all options

**Overview**

Below is a list of configured DDNS configurations and their current state.  
If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns\_ipv4' and 'myddns\_ipv6'  
[To change global settings click here](#)

Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
myddns_ipv4	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	Never Disabled	<input type="text"/>	<a href="#">Edit</a> <a href="#">Delete</a>
myddns_ipv6	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	Never Disabled	<input type="text"/>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="text"/>		<input type="checkbox"/>			<a href="#">Add</a>

[Reset](#) [Save](#) [Save & Apply](#)

**Dynamic DNS** Click this link to show information about the current DDNS version.

### Hints

**Show More** Click this link to show hints on how to optimize your DDNS.

### Overview

**To global settings click here** Click to access DDNS global settings.

**Configuration** Displays the DDNS Configuration Name.

**Hostname/Domain Registered IP** Displays the Hostname and Domains Registered IP.

**Enabled** Tick to enable / disable the DDNS configuration.

**Last Update / Next Update** Displays when the last DDNS update was / when the next DDNS update is.

**Process ID Start / Stop** Click to start the DDNS Process ID.

## Global Settings

### Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

#### Global Settings

Configure here the details for all Dynamic DNS services.  
**It is NOT recommended for casual users to change settings on this page.**

Allow non-public IP's	<input type="checkbox"/> Non-public and by default blocked IP's: <b>IPv4:</b> 0/8, 10/8, 100.64/10, 127/8, 169.254/16, 172.16/12, 192.168/16 <b>IPv6:</b> ::1/32, f000::/4
Date format	<input type="text" value="%F %R"/> <input checked="" type="checkbox"/> Use C++ date format characters here Current setting: <b>2021-10-19 11:18</b>
Status directory	<input type="text" value="/var/run/ddns"/> <input checked="" type="checkbox"/> Directory contains PID and other status information for each running section
Log directory	<input type="text" value="/var/log/ddns"/> <input checked="" type="checkbox"/> Directory contains Log files for each running section
Log length	<input type="text" value="250"/> <input checked="" type="checkbox"/> Number of last lines stored in log files

[Back to Overview](#) [Reset](#)

[Save](#) [Save & Apply](#)

**Allow Non-public IP's** Tick to allow Non-Public IP Addresses.

**Date Format** Input date format code.

**Status Directory** Input device location of status directory.

**Log Directory** Input device location of log directory.

**Log Length** Number of lines stored in log files.

Add DDNS / Edit DDNS

**Dynamic DNS**

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

**Details for: myddns\_ipv4**

Configure here the details for selected Dynamic DNS service.  
 For detailed information about parameter settings look here.

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
Enabled	<input type="checkbox"/> ⓘ If this service section is disabled it could not be started. Neither from LuCI interface nor from console		
IP address version	<input checked="" type="radio"/> IPv4-Address <input type="radio"/> IPv6-Address ⓘ Defines which IP address 'IPv4/IPv6' is send to the DDNS provider		
DDNS Service provider [IPv4]	-- custom --		
Custom update-URL	silvernet-ddns.com ⓘ Update URL to be used for updating your DDNS Provider. Follow instructions you will find on their WEB page.		
Custom update-script	<input type="text"/> ⓘ Custom update script to be used for updating your DDNS Provider.		
Hostname/Domain	silvernet.com ⓘ Replaces [DOMAIN] in Update-URL		
Username	silvernetddns ⓘ Replaces [USERNAME] in Update-URL		
Password	<input type="password"/> ..... ⓘ Replaces [PASSWORD] in Update-URL		

[Back to Overview](#) [Reset](#)

[Save](#) [Save & Apply](#)

**Enabled** Tick to enable specified DDNS section.

**IP Address Version** Choose which Internet Protocol version to use for your DDNS.

**DDNS Service Provider [IPv4]** Choose which DDNS service provider to use.

**Custom Update-URL** Input DDNS Update URL from DDNS provider.

**Custom Update-Script** Input custom DDNS update script for updating DDNS provider.

**Hostname/Domain** Input hostname / domain instead of typing into Custom Update-URL.

**Username** Input Username for custom update URL instead of typing into Custom Update-URL.

**Password** Input Password for custom update URL instead of typing into Custom Update-URL.

## Advanced Settings

**Dynamic DNS**

### Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

**Details for: silvernet**

Configure here the details for selected Dynamic DNS service.  
[For detailed information about parameter settings look here.](#)

<p>Basic Settings   <b>Advanced Settings</b>   Timer Settings   Log File Viewer</p>	
IP address source [IPv4]	<p>Network</p> <p>Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider</p>
Network [IPv4]	<p>wan</p> <p>Defines the network to read systems IPv4-Address from</p>
DNS-Server	<p>silvernet.lan</p> <p>OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'.                  Format: IP or FQDN</p>
PROXY-Server	<p>silver.net@silvernetproxy.lan:00</p> <p>OPTIONAL: Proxy-Server for detection and updates.                  Format: [user:password@]proxyhost:port                  IPv6 address must be given in square brackets: [2001:db8::1]:8080</p>
Log to syslog	<p>Notice</p> <p>Writes log messages to syslog. Critical Errors will always be written to syslog.</p>
Log to file	<p><input checked="" type="checkbox"/></p> <p>Writes detailed messages to log file. File will be truncated automatically.                  File: "/var/log/ddns/silvernet.log"</p>

[Back to Overview](#) [Reset](#)

[Save](#) [Save & Apply](#)

**IP Address Source [IPv4/6]** Defines the source to read systems IPv4-Addresses from, that will be sent to the DDNS provider.

**Network [IPv4/6]** Defines the interface to read systems IP Addresses from.

**DNS-Server** Input non-default DNS Server to detect registered IP Addresses.

**PROXY-Server** Input Proxy server for DDNS detection and updates.

**Log to Syslog** Specify which type of log to write to the system log.

**Log to File** Tick to enable detailed logging messages.



## Timer Settings

SILVERNET MICRO | v2.1.3(170821)

Unsaved Changes: 2

Status Admin **Services** Network Logout

Dynamic DNS

### Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

#### Details for: silvernet

Configure here the details for selected Dynamic DNS service.  
[For detailed information about parameter settings look here.](#)

Basic Settings	Advanced Settings	Timer Settings	Log File Viewer
<p><b>Check Interval</b></p> <p>10 <input type="text"/> minutes</p> <p>Interval to check for changed IP                      Values below 5 minutes == 300 seconds are not supported</p>			
<p><b>Force Interval</b></p> <p>72 <input type="text"/> hours</p> <p>Interval to force updates send to DDNS Provider                      Setting this parameter to 0 will force the script to only run once                      Values lower 'Check Interval' except '0' are not supported</p>			
<p><b>Error Retry Counter</b></p> <p>0 <input type="text"/></p> <p>On Error the script will stop execution after given number of retrys                      The default setting of '0' will retry infinite.</p>			
<p><b>Error Retry Interval</b></p> <p>60 <input type="text"/> seconds</p> <p>On Error the script will retry the failed action after given time</p>			

[Back to Overview](#) [Reset](#)

[Save](#) [Save & Apply](#)

**Check Interval** Specify interval to check for changed IP address.

**Force Interval** Specify interval to force updates from DDNS provider.

**Error Retry Counter** Specify number of attempts before DDNS script will stop execution.

**Error Retry Interval** Specify interval in which DDNS script will retry after Error Counter.

## Log File Viewer

**SILVERNET** MICRO | v2.1.3(170821) Unsaved Changes: 4

Status Admin Services Network Logout

Dynamic DNS

**Dynamic DNS**

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

**Details for: myddns\_ipv4**  
Configure here the details for selected Dynamic DNS service.  
[For detailed information about parameter settings look here.](#)

Basic Settings Advanced Settings Timer Settings **Log File Viewer**

Read / Reread log file

```
/var/log/ddns/myddns_ipv4.log
Please press [Read] button
```

Basic Settings Advanced Settings Timer Settings **Log File Viewer**

Read / Reread log file

```
121225 : *****
121225 note : PID '715' started at 2021-05-19 12:12
121225 : uci configuration:
ddns.myddns_ipv4.domain='yourhost.example.com'
ddns.myddns_ipv4.enabled='0'
ddns.myddns_ipv4.interface='wan'
ddns.myddns_ipv4.ip_network='wan'
ddns.myddns_ipv4.ip_source='network'
ddns.myddns_ipv4.password='your_password'
ddns.myddns_ipv4.service_name='dyndns.com'
ddns.myddns_ipv4.username='your_username'
ddns.myddns_ipv4=service
121226 : ddns version : 2.4.3-2
121226 : verbose mode : 0 - run normal, NO console output
121226 WARN : Service section disabled! - TERMINATE
121226 WARN : PID '715' exit WITH ERROR '1' at 2021-05-19 12:12
```

**Read / Reread log file** Click to display current system log file.

## NETWORK TAB

The Network tab contains everything needed to set up the networking part of the link. This includes:

- **LAN Interface:** This allows you to configure the IP Address settings, DHCP Server Settings, DNS Settings, Firewall Settings and Physical settings.
- **Wireless Settings:** This allows you to configure settings such as Country Codes, Channel Selection, ACS Scanning, Antenna Gain, Transmit Power, Interface Configuration, Wireless Security, MAC-filtering, Multipoint Enhancement Settings, Distance Settings, Adaptive Noise Immunity, Chainmask Selection, Dynamic Channel Selection.
- **VLANs:** This allows you to enable and manage VLANs.

The screenshot shows the SilverNet web interface. At the top left is the SilverNet logo and version information: MICRO | v2.1.3(170821) | Auto Refresh: on. On the top right, it says 'Changes: 0'. Below the logo is a navigation menu with 'Status', 'Admin', 'Services', 'Network', and 'Logout'. Under 'Network', there are sub-menus for 'Interfaces', 'Wireless', 'VLAN', and 'Diagnostics'. The 'Interfaces' section is active, showing an 'Interface Overview' table. The table has two columns: 'Network' and 'Status'. There is one entry for 'LAN' with a green status bar. To the right of the table are 'Actions' buttons: 'Connect', 'Stop', 'Edit', and 'Delete'. Below the table is a button that says 'Add new interface...'. The LAN interface details shown are: Uptime: 1d 1h 43m 59s, MAC-Address: 50:11:EB:00:B2:0C, RX: 200.44 MB (1993304 Pkts.), TX: 9.14 MB (41068 Pkts.), and IPv4: 192.168.168.215/24.

**Note** Click the edit button to enter the set-up page for LAN or WLAN interface.

## LAN INTERFACE

**SILVERNET** MICRO | v2.1.3(170821) | Auto Refresh: on Changes: 0

Status Admin Services **Network** Logout

**Interfaces** Wireless VLAN Diagnostics

### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

#### Common Configuration

General Setup	Advanced Settings	Physical Settings
<b>Status</b> <div style="float: right;"> <b>Uptime:</b> 1h 11m 35s  <b>MAC-Address:</b> 50:11:EB:00:BD:04  <b>RX:</b> 4.92 MB (46301 Pkts.)  <b>TX:</b> 2.74 MB (5263 Pkts.)  <b>IPv4:</b> 192.168.168.228/24                 </div>		
Protocol	Static address	
IPv4 address	192.168.168.228	
IPv4 netmask	255.255.255.0	
IPv4 gateway		
IPv4 broadcast		
Use custom DNS servers		

#### DHCP Server

General Setup
Ignore interface <input checked="" type="checkbox"/> <input type="checkbox"/> Disable DHCP for this interface.

[Back to Overview](#) [Reset](#)

[Save](#) [Save & Apply](#)

## General Setup

**Protocol** 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 configured on your network for this to function.

**Static** Allows you to enter a static IP address.

**IPv4 Address** Enter the IP address you wish to give to the device. You will use this IP address to access the device interface.

**IPv4 Netmask** Enter the class for the IP address. The default is a class C value of 255.255.255.0

**IPv4 Gateway** (optional) Enter the gateway IP address of the network the device is connected to.

**IPv4 Broadcast** (optional) Specifies the IPv4 broadcast address

**Use Custom DNS Servers** Enter the IP address for the DNS server you wish to use

## DHCP SERVER

**DHCP Server** disabled if ticked, un-tick to enable.

### DHCP Server

General Setup	Advanced Settings
Ignore interface	<input type="checkbox"/> <b>Disable DHCP</b> for this interface.
Start	<input type="text" value="100"/> <b>Lowest leased address as offset from the network address.</b>
Limit	<input type="text" value="150"/> <b>Maximum number of leased addresses.</b>
Leasetime	<input type="text" value="12h"/> <b>Expiry time of leased addresses, minimum is 2 Minutes (2m).</b>

### DHCP Server

General Setup	Advanced Settings
Dynamic DHCP	<input checked="" type="checkbox"/> <b>Dynamically allocate DHCP addresses for clients.</b> If disabled, only clients having static leases will be served.
Force	<input type="checkbox"/> <b>Force DHCP on this network even if another server is detected.</b>
IPv4-Netmask	<input type="text"/> <b>Override the netmask sent to clients. Normally it is calculated from the subnet that is served.</b>
DHCP-Options	<input type="text"/> <b>Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.</b>

**DHCP Server** The device will act as a DHCP server hand out IP addresses automatically.

**Start** Specifies the lowest leased address to be issued

**Limit** Sets the maximum number of leased addresses

**Leasetime** States the expiry time of leased addresses

**Dynamic DHCP** Dynamically allocates DHCP addresses for clients. If disabled, only clients having static leases will be served.

**Force** Forces DHCP on this network even if another server is detected

**IPv4 Netmask** Overrides the netmask sent to clients. Normally it is calculated from the subnet that is served.

**DHCP Options** Defines additional DHCP options, for example "6, 192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients. Normally, connected devices would take this board's IP address as the default gateway. To set an alternative default gateway, add the DHCP option "3, 192.168.2.3" for example.

## Advanced Settings

**SILVERNET** MICRO | v2.1.3(170821) | Auto Refresh: **on** Changes: 0

Status Admin Services **Network** Logout

**Interfaces** Wireless VLAN Diagnostics

### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANID (e.g.: eth0.1).

**Common Configuration**

General Setup	Advanced Settings	Physical Settings
Override MAC address	<input type="text" value="50:11:EB:00:BD:04"/>	
Override MTU	<input type="text" value="1500"/>	
Use gateway metric	<input type="text" value="0"/>	

**Bring up on boot** Tick to enable this interface on device boot.

**Use built in IPv6-Management** Tick to enable usage of built in IPv6 management for this interface.

**Override MAC Address** Allows you to specify a different MAC address other than the routers original one. This is useful if the ISP uses Mac addresses of routers to identify customers.

**Override MTU** Sets the maximum transmission unit (MTU), the default being 1500 bytes, we recommend you do not change this unless your ISP requires you to.

**Use Gateway Metric** Allows you to specify a gateway metric. When a connected device must choose from multiple gateways, the gateway with the smallest/lowest metric is chosen.

## Physical Settings

SILVERNET

MICRO | v2.1.3(170821) | Auto Refresh: on

Changes: 0

Status Admin Services **Network** Logout

**Interfaces** Wireless VLAN Diagnostics

### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

#### Common Configuration

General Setup	Advanced Settings	Physical Settings
Bridge interfaces		<input checked="" type="checkbox"/> creates a bridge over specified interface(s)
Enable STP		<input type="checkbox"/> Enables the Spanning Tree Protocol on this bridge
Interface	<input type="checkbox"/> Ethernet Adapter: "bond0" <input checked="" type="checkbox"/> Ethernet Adapter: "eth0" ( <a href="#">lan</a> ) <input type="checkbox"/> VLAN Interface: "eth0.1" <input type="checkbox"/> VLAN Interface: "eth0.2" <input checked="" type="checkbox"/> Ethernet Adapter: "eth1" ( <a href="#">lan</a> ) <input type="checkbox"/> Ethernet Adapter: "gretap0" <input type="checkbox"/> Ethernet Adapter: "ip6tnl0" <input type="checkbox"/> Ethernet Adapter: "miireg" <input type="checkbox"/> Ethernet Adapter: "teqj0" <input checked="" type="checkbox"/> Wireless Network: Client "silvernet-manual" ( <a href="#">lan</a> ) <input type="checkbox"/> Custom Interface: <input type="text"/>	

**Bridge Interfaces** Tick to enable bridging of ticked interfaces.

**Enable STP** Enables the Spanning Tree Protocol on this unit. This is disabled by default

The Spanning Tree Protocol (STP) is a network protocol. The main purpose of **STP** is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.

**Interface** List of all Interfaces and Adapters on device, tick to enable bridging between if Bridge Interfaces is enabled.

## WIRELESS INTERFACE

**SILVERNET** MICRO | v2.1.3(170821) | Auto Refresh: on Changes: 0

Status Admin Services **Network** Logout

Interfaces **Wireless** VLAN Diagnostics

### Wireless Overview

**Interface (wi0)**  
 Channel: 116 (5.580 GHz) | Bitrate: 300 Mbit/s

SSID: silvernet-manual | Mode: Master WDS  
 BSSID: 50:11:EB:00:B8:9F | Encryption: WPA2 NONE (CCMP)

### Associated Stations

SSID	MAC-Address	IPv4-Address	Noise	Rssi	RX Rate	TX Rate	TxCCQ	Up Time
silvernet-manual	50:11:EB:00:BD:07	Static IP	-95 dBm	64(64,60,0)	300.0 Mbit/s	300.0 Mbit/s	93%	1 hours 4 s

## Spectrum scans

### Wireless Overview

**5GHz Radio**  
 Channel: 36 (5.180 GHz) | Bitrate: 270 Mbit/s

SSID: silvernetwireless | Mode: Client-WDS  
 BSSID: 50:11:EB:00:74:A5 | Encryption: WPA2 PSK (AUTO)

Status Admin Services **Network** Logout

Interfaces Wireless **VLANs**

### Join Network: Wireless Scan

	<b>SilverNet1</b> Channel: 140   Mode: Master   BSSID: 50:11:EB:10:13:B0   Encryption: open	<input type="button" value="Join Network"/>
	<b>SilverNet1</b> Channel: 60   Mode: Master   BSSID: 50:11:EB:10:17:28   Encryption: open	<input type="button" value="Join Network"/>
	<b>silvernetwireless888</b> Channel: 149   Mode: Master   BSSID: 50:11:EB:00:6F:62   Encryption: WPA2 - PSK	<input type="button" value="Join Network"/>
	<b>silvernetwireless</b> Channel: 36   Mode: Master   BSSID: 50:11:EB:00:74:A5   Encryption: WPA2 - PSK	<input type="button" value="Join Network"/>
	<b>silvernetwireless4321</b> Channel: 161   Mode: Master   BSSID: 50:11:EB:00:6E:6E   Encryption: WPA2 - PSK	<input type="button" value="Join Network"/>
	<b>SilverNet</b> Channel: 116   Mode: Master   BSSID: 14:1F:BA:7D:80:84   Encryption: WPA2 - PSK	<input type="button" value="Join Network"/>

Click the **Scan** button to perform a spectrum scan from the Station

This will show you a list detailing the channel number, MAC address and encryption method of any device nearby. You can click the "Join Network" button to connect to a specific AP.

From the Wireless Overview page, click the edit button to enter the wireless page



## DEVICE CONFIGURATION

**SILVERNET** MICRO | v2.1.3(170821) | Auto Refresh: on Changes: 0

Status Admin Services **Network** Logout

Interfaces **Wireless** VLAN Diagnostics

### Wireless Network: Master "silvernet-manual" (ath0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

**Device Configuration**

General Setup | **Advanced Settings**

**Status**

**Mode:** Master WDS | **SSID:** silvernet-manual  
**BSSID:** 50:11:EB:00:B8:9F | **Encryption:** WPA2 NONE (CCMP)  
**Channel:** 108 (5.540 GHz) | **Tx-Power:** 16 dBm  
**Signal:** -33 dBm | **Noise:** -95 dBm  
**Bitrate:** 300.0 Mbit/s | **Country:** United Kingdom B

Wireless network is enabled  Disable

Country Code United Kingdom Band B  
Ensure you choose the correct country of operation to comply with local legal requirements.

Mode 300 Mbps Max

Channel Spectrum Width 40MHz 2nd channel above

Frequency auto

Block Dfs Channel list   Block Dfs Channel list

Background ACS scan   Automatically scan and switch to best channel after a period of time, default is 60 seconds

Scan List:

Enable Scan List

100 (5.500 GHz)  108 (5.540 GHz)  116 (5.580 GHz)  124 (5.620 GHz)

132 (5.660 GHz)

Antenna Gain (dBi) 14

Transmit Power Max  
 Max EIRP: 30, Max Single Chain EIRP: 27

**Status** This shows the current wireless connectivity of the device, similar to the “Status Tab”.

**Wireless Network is Enabled** Enabled by default, click to disable wireless interface.

**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.

**Mode** Choose what throughput speeds to limit the wireless communication to. This can be upgraded via License Keys to 866Mbps.

**Channel Spectrum Width** Displays the spectral width of the radio channel. You can use this option to control the bandwidth consumed by your link. Using higher Channel width increases throughput. Using lower Channel width reduces throughput.

Channel widths available are **5 MHz, 10 MHz, 20 MHz, and 40 MHz**

When the 802.11ac wireless standard is used, the 80 MHz band can be selected. An 80 MHz band can carry twice the amount of data of a 40 MHz band.

**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 30 minutes to connect.

**Block DFS Channel List** Tick to block selection of DFS channels to avoid DFS radar interference.

**Background ACS Scan / ACS Scan Interval** This will allow the device to automatically scan and switch to a better channel after a period of time when no client is connected. Default time for the scan is every 60 seconds.

ACS provides an easy way to optimise channel arrangement. It provides an optimal solution only if it is used on all APs in a site. Using ACS on a single AP provides a useful but sub-optimal solution. Once an AP has selected a channel, it remains operating on that channel until the user changes the channel or it scans again (after a reboot). The best way to make the AP always choose the best channel is to enable Dynamic Channel Selection (see below)

**Antenna Gain** Represents the gain relative to an isotropic antenna. A higher antenna gain results in the transmit power more focused towards a certain direction. You can set this depending on the antenna you have, e.g. PICO 12dBi, MICRO 15dBi, LITE 18dBi, MAX 25dBi. When country code is set, the value of the antenna gain will be considered to limit the selectable transmit power, such that the EIRP limits of the country are satisfied.

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

## 5MHz and 10MHz Channel Spectrum Width

From the Channel Spectrum Width drop down list, choose 20MHz. A new setting will appear, Channel Bandwidth Used. Select either 20MHz, 10MHz or 5MHz from this new drop-down menu.

Click Save & Apply to save the configuration.

**Device Configuration**

General Setup | **Advanced Settings**

Status 100%

**Mode:** Master WDS | **SSID:** silvernet-manual  
**BSSID:** 50:11:EB:00:B2:0F | **Encryption:** WPA2 NONE (CCMP)  
**Channel:** 132 (5.660 GHz) | **Tx-Power:** 30 dBm  
**Signal:** -39 dBm | **Noise:** -95 dBm  
**Bitrate:** 300.0 Mbit/s | **Country:** NA

---

Wireless network is enabled Disable

---

Country Code No Country

Ensure you choose the correct country of operation to comply with local legal requirements.

---

Mode 300 Mbps Max

---

Channel Spectrum Width 20MHz

---

Channel Bandwidth Used 20 MHz

20 MHz  
10 MHz  
5 MHz

---

Block Dfs Channel list Block Dfs Channel list

---

Background ACS scan  Automatically scan and switch to best channel after a period of time, default is 60 seconds

---

Antenna Gain (dBi) 0

---

Transmit Power Max

Max EIRP: 50, Max Single Chain EIRP: 47

Using higher bandwidth increases throughput. Using lower bandwidth reduces throughput.

Channel widths available are:

**5 MHz – TX 32 – 20/25Mbps**

**10 MHz – TX 65 – 40/45Mbps**

**20 MHz – TX 130 – 90/95Mbps**

**20/40 MHz – TX 300 – 90/95Mbps – Both ways**

## Advanced settings

SILVERNET MICRO | v2.1.3(170821) | Auto Refresh: on Changes: 0

Status Admin Services **Network** Logout

Interfaces **Wireless** VLAN Diagnostics

### Wireless Network: Master "silvnet-manual" (ath0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

#### Device Configuration

General Setup	Advanced Settings
Link Distance	<input type="text" value="2000"/> <small>in metres, leave blank for auto.</small>
Adaptive noise immunity	<input checked="" type="checkbox"/> <small>Controls radio sensitivity in the face of noise sources</small>
Dynamic channel selection	<input type="text" value="Disable"/> <small>Automatically switches channel to avoid interference</small>

**Link Distance** Specifies the distance between the AP and the station if the previous option is unchecked. Min: 300, Max: 24000 (40MHz), 48000 (20MHz). This value should be set to slightly more than the physical distance between the AP and the farthest station. Leave blank for auto.

**Adaptive 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.

**Dynamic Channel Selection** This is a feature to monitor traffic and noise levels. If the noise levels exceed the threshold, the AP will disconnect any associated stations and move to a new channel. The stations are expected to re-associate with the AP on their own. Available selections are:

- **Look for CW Interference** Use this feature to detect and avoid continuous wave (CW) interference.
- **Look for WLAN Interference** Use this feature to detect and avoid wireless interference
- **Look for CW and WLAN Interference** Use this feature to detect and avoid continuous wave (CW) interference and Wireless interference.

## Interface Configuration

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
ESSID	silvernet-manual		
Mode	Access Point (WDS) ▼		
Guard Interval	Short ▼		
Data Rate (Mbps)	Auto ▼		
Hide ESSID	<input type="checkbox"/>		

**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.

**Mode** Displays the operating mode of the radio interface. The Pro Range supports four operating modes:

- Station
- Station WDS
- Access Point
- Access Point WDS

**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. Multiple stations or Stations WDS can connect to an AP WDS.

**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.**

**Guard Interval** This is the space between symbols being transmitted. The Guard Interval is there to eliminate inter-symbol interference. For long distance connections, select Long to give better performance.

**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

The MCS settings have different rates depending on the Chainmask Selection (see above for Chainmask Selection) that is used.

	Chainmask Selection	
	1x1	2x2
<b>MCS0</b>	13.5Mbps	27Mbps
<b>MCS1</b>	27Mbps	54Mbps
<b>MCS2</b>	40.5Mbps	81Mbps
<b>MCS3</b>	54Mbps	108Mbps
<b>MCS4</b>	81Mbps	162Mbps
<b>MCS5</b>	108Mbps	216Mbps
<b>MCS6</b>	121.5Mbps	243Mbps
<b>MCS7</b>	135Mbps	300Mbps

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

**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 and Access Point WDS mode.

## WIRELESS SECURITY

### Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption	WPA2-PSK		
Cipher	Auto		
Key	<input type="password" value="••••••••"/>		

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:

**No Encryption** If you want an open network without wireless security, select No Encryption.

**WEP Open System** WEP (Wired Equivalent Privacy) is the oldest and least secure security algorithm.

**WEP Shared Key** WEP (Wired Equivalent Privacy) with slightly better authentication.

**WPA-PSK** WPA (Wi-Fi Protected Access) was developed as a stronger encryption method than WEP. This uses TKIP Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

**WPA2-PSK** WPA2 was developed to strengthen wireless encryption security and is stronger than WEP and WPA. **This is the most secure option.** It uses the latest Wi-Fi encryption standard, and the latest AES (Advanced Encryption Standard) encryption protocol.

**WPA2-PSK AES+** As above but with 256bit encryption.

**WPA-PSK/WPA2-PSK Mixed Mode** This enables both WPA and WPA2 with both TKIP and AES. This provides maximum compatibility with any ancient devices you might have.

**IEEE802.1X/WPA-EAP** This will require the equipment to be authenticated via a RADIUS server. The RADIUS server must support EAP or be chained/proxied to one that does.

**IEEE802.1X/WPA2-EAP** This will require the equipment to be authenticated via a RADIUS server. The RADIUS server must support EAP or be chained/proxied to one that does.

## WEP

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

**Encryption** Select the type of encryption you want to use.

**Open System** (Default) No authentication. We recommend using this option over shared authentication.

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

**Used Key Slot** Select which key to use

**Key #1** Enter a security key to use

**Key #2** Enter a security key to use


**Key #3** Enter a security key to use

**Key #4** Enter a security key to use

## WPA/WPA2 Authentication

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

### Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption	WPA2-PSK ▼		
Cipher	Auto ▼		
Key	<input type="password" value="....."/> 		

**Cipher** Specify which of the following to use:

- **Auto** – Uses the most appropriate algorithm for the network
- **CCMP (AES)** - Advanced Encryption Standard (AES) algorithm. **(default)**
- **TKIP and CCMP (AES)** - Temporal Key Integrity Protocol which uses RC4 encryption algorithm and Advanced Encryption Standard (AES) algorithm.
- 

**Key** The key is an alpha-numeric password between 8 and 63 characters long.



## MAC-Filter

This setting is only available on the Access Point.

**Interface Configuration**

General Setup | Wireless Security | **MAC-Filter** | Advanced Settings

MAC-Address Filter	Allow all except listed
MAC-List	00:00:00:00:00:00

**MAC-Address Filter** Lets you allow only devices with the listed MAC address to associate with this AP, or lets you block devices with the listed MAC address.

**Mac List** Adds the MAC address of the remote device to either block or allow.

## Advanced Settings

**Interface Configuration**

General Setup | Wireless Security | MAC-Filter | **Advanced Settings**

Station Isolation	<input type="checkbox"/> Prevents client-to-client communication
Block VLAN passthrough	<input type="checkbox"/> Prevents tagged VLAN traffic from passing across the link
RTS/CTS Threshold	<input type="text"/>
Minimum Received Signal	<input type="text"/> Minimum SNR in dB
WMM Mode	<input checked="" type="checkbox"/>

**Station Isolation** When checked, it prevents station-to-station communication. When Station Isolation is disabled, wireless clients can communicate with one another normally by sending traffic through the AP. When Station Isolation is enabled, the AP blocks communication between wireless clients on the same AP.

**Block VLAN Passthrough** Tick to block VLAN traffic from passing across the link.

**RTS/CTS Threshold** This value is set to **2346 as default**, which is the maximum 802.11 packet size. We recommend leaving this setting for Point-to-Point links, however, for Multipoint setups we recommend setting the RTS Threshold lower (538). The AP device sends Request to Send (RTS) frames to a 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. The CTS contains a hold off time that prevents other clients from sending anything whilst the targeted client sends its data. Setting the RTS lower will improve the stability of a Multipoint setup.

**Minimum Received Signal** Input a numeric value in dB for the minimum allowed SNR to establish a link.

**WMM Mode** Provides Quality of Service (QoS) features. This is checked by default. Wireless multimedia (WMM) enables the classification of the network traffic into 4 main types, voice, video, best effort, and background, in decreasing order of priority. Higher priority traffic has a higher transmission opportunity and would have to wait less time to transmit. As a result, an existing video stream would not be interrupted by additional background processes.

## VLANS

The VLANS tab contains everything needed to set up VLANS.

**SILVERNET** MICRO | v2.1.3(170821) | Auto Refresh: on Changes: 0

Status Admin Services **Network** Logout  
 Interfaces Wireless **VLAN** Diagnostics

### VLAN

The network ports on this device can be combined to several **VLANS** in which computers can communicate directly with each other. **VLANS** are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

**VLAN Operation**

Enable VLAN functionality

**VLAN Configuration**

VLAN ID	Ethernet	Port 1	Port 2	Port 3	Port 4	Wireless	Port 6	
1	1000baseT full-duplex	no link	no link	no link	no link	100baseT full-duplex		
	tagged	untagged	untagged	untagged	untagged	off	off	Delete
2		off	off	off	off	untagged	off	Delete
Add								

Reset Save Save & Apply

**Enable VLAN Functionality** Check to enable VLANS

## VLAN Entries

### VLANs on "switch0"

VLAN ID	CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	
Port status:	100baseT full-duplex	no link	no link	no link	no link	100baseT full-duplex		
1	tagged	untagged	untagged	untagged	untagged	off	off	Delete
2	tagged	off	off	off	off	untagged	off	Delete
Add								

**VLAN ID** Enter the VLAN ID you wish to use

**CPU** Choose to leave off, or Tag or Untag the Ethernet interface

**Port 1** Choose to leave off, or Tag or Untag the Port 1 interface

**Port 2** Choose to leave off, or Tag or Untag the Port 2 interface

**Port 3** Choose to leave off, or Tag or Untag the Port 3 interface

**Port 4** Choose to leave off, or Tag or Untag the Port 4 interface

**Port 5** Choose to leave off, or Tag or Untag the Wireless interface

**Port 6** Choose to leave off, or Tag or Untag the Port 6 interface

**Delete** Delete the VLAN

## DIAGNOSTICS

**SILVERNET** MICRO | v2.1.3(170821) Changes: 0

Status Admin Services **Network** Logout

Interfaces Wireless VLAN **Diagnostics**

### Diagnostics

**Network Utilities**

www.silvernet.com	www.silvernet.com	www.silvernet.com
IPv4 ▾ <input type="checkbox"/> Ping	<input type="checkbox"/> Traceroute	<input type="checkbox"/> Nslookup

Use this page to perform some basic network diagnostic tests, such as Ping, Traceroute and Nslookup.

**Ping** Enter an address to Ping, as well as the Internet Protocol Type. Ping is a command-line utility that acts as a test to see if a networked device is reachable. The ping command sends a small amount of data over the network to a specific device and measures the round-trip time to receive a response.

**Traceroute** Enter an address to traceroute. Traceroute is a diagnostic command for displaying possible routes and measuring transit delays of packets across a network. The history of the route is recorded as the round-trip times of the packets received from each successive host in the route; the sum of the mean times in each hop is a measure of the total time spent to establish the connection. Traceroute proceeds unless all (usually three) sent packets are lost more than twice; then the connection is lost and the route cannot be evaluated.

**Nslookup** Enter an address to query. Nslookup is a network administration command-line tool for querying the DNS to obtain domain name or IP address mapping, or other DNS records.

## STANDARDS

### DECLARATION OF CONFORMITY

SilverNet Limited declares the following:

Product Name: PRO Range GEN4

Model No.: PICO, MICRO, LITE, MAX conforms to the following Product Standards:

This device complies with the Electromagnetic Compatibility Directive (89/336/EEC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards.)

**Electromagnetic Interference (Conduction and Radiation):** EN 55022 (CISPR 22)

**Electromagnetic Immunity:** EN 55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)

**Low Voltage Directive:** EN 60 950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11: 1997.

**Therefore, this product is in conformity with the following regional standards:**

**FCC Class B:** following the provisions of FCC Part 15 directive,

**CE Mark:** following the provisions of the EC directive.

SilverNet Limited also declares that:

The wireless card in this product complies with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following:

**EMC Standards:** FCC: 47 CFR Part 15, Subpart B, 47 CFR Part 15, Subpart C (Section 15.247);

CE: EN 300 328-2, EN 300 826 (EN 301 489-17)

**Therefore, this product is in conformity with the following regional standards:**

**FCC Class B:** following the provisions of FCC Part 15 directive,

**CE Mark:** following the provisions of the EC directive.

## WARNINGS

### RADIO FREQUENCY INTERFERENCE REQUIREMENTS

The operation of this device in the 5.15 GHz to 5.25 GHz frequency range is restricted to indoor use. FCC regulations require this product to be used indoors while operating at 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference. However, the operation of this device in the 5.25 GHz to 5.35 GHz frequency range is allowed for both indoor and outdoor use. High power radars are allocated as primary users of the 5.25 GHz to 5.35 GHz and 5.65 GHz to 5.85 GHz bands. These radar stations can cause interference with and/or damage to this device.

#### FCC Warning

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

- Reorient or relocate the radio/TV receiving antenna.
- Increase the separation between the equipment and the radio/TV receiver.
- Connect the equipment into an outlet on a circuit different from that to which the radio/TV receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help. Modifications made to the product, unless expressly approved by SilverNet Limited, could void the user's authority to operate the equipment.

#### RF Exposure Requirements

To ensure compliance with FCC RF exposure requirements, the antenna used for this device must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or radio transmitter. Installers and end-users must follow the installation instructions provided in this user guide.

## CE Statement

The PRO Range GEN4 is intended to be used by suitably trained individuals or organisations that are familiar with the requirements of the R&TTE directive. In particular the client must ensure that appropriate antennas and transmit power levels are selected to ensure that all power limits are met. Hereby, SilverNet Limited declares that this device is in compliance with the essential requirements and other relevant provisions of the R&TTE Directive 1999/5/EC. However, the use of the following warning symbol



Means that this equipment is subject to restrictions of use in certain countries and selection of the correct country of operation (country code) will ensure that the device operates only on the frequencies permissible within that country. It is also the operator's responsibility to ensure that appropriate licenses have been sought when operating on licensed frequencies, for example UK Band C, 5725-5850MHz.

In the UK, all radios operate under the control of Ofcom. Radio use in the 2.4 & 5GHz bands are deemed to be Licence Exempt with the exception of Band C. Band C (5.725 to 5.825GHz) requires registration with Ofcom under a light licensing scheme. While this band is still effectively licence exempt, Ofcom wants to keep a register of all FWA links and charges a small fee. Any user wishing to set up an outdoor link for FWA needs to apply to Ofcom for a site license; the licence is not hard to obtain and is only £50 which includes registration of up to 50 terminals. For every terminal beyond 50 you should add £1 to the cost of your licence.

Further information on the legal implications of Band C usage can be found on the Ofcom website.

## TROUBLESHOOTING

If you are having problems with your links, then please check the following before calling our support team.

**Line of Sight** The radios work best when they have line-of-sight. If the radios do not have line-of-sight, then you will get a very poor signal or no signal at all.

**Alignment** If the radios are not correctly aligned the signal quality of the radios will suffer and you may not receive the throughput you require. Run SilverView and use the data test tool.

**Power** If the units are not powering on then you will need to test the Ethernet cable and re-terminate it if required. We recommend outdoor shielded grade cable for all installations. Please also check that the PSU is plugged in and turned on.

**Interference** Our radios use auto-channel select and should avoid interferences as best as possible. Rebooting the radios will allow a re-scan. If you are experiencing interference problems when using the radios, try setting them on a static channel. Try each channel until you find one that gives you a better signal. Use SilverView and run a data test.

## WARRANTY

The PRO Range GEN4 comes with a 2-year warranty as standard. For full terms and conditions of warranty please go to [www.silvernet.com/terms-and-conditions/](http://www.silvernet.com/terms-and-conditions/)

## CONTACT SILVERNET

Email us at [support@silvernet.com](mailto:support@silvernet.com)

Call our support team on **08712233067**

[www.silvernet.com](http://www.silvernet.com)

## COPYRIGHT INFORMATION

Copyright ©2021 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.



## OTHER SILVERNET PRODUCTS

### PRO RANGE



### INDUSTRIAL NETWORK TRANSMISSION



### INTELLIGENT WI-FI SOLUTIONS



### INDUSTRY LEADING TECHNICAL SUPPORT

