

SILVERNET

WIRELESS-NETWORK-SOLUTIONS

PRO RANGE G5



MICRO



LITE



BASE

User Manual

TABLE OF CONTENTS

Introduction.....	5
Supported Products.....	5
Wireless Modes	5
System Requirements.....	5
Packing list	6
The Enclosure and LED indicators	7
Configuration.....	8
Getting Started	8
Setup Wizard	9
Status.....	12
Overview.....	12
System	13
Wireless	13
Associated Stations.....	14
Network.....	15
Routing	16
ARP (Address Resolution Protocol)	16
Active IPv4 Routes	16
Network.....	17
Network.....	17
LAN	18
VLAN	18
TR069.....	23
SNMP	24
Wireless.....	27
Wireless.....	27

<i>Wireless Configuration</i>	28
<i>Antenna Gain</i>	29
<i>2.4G Wireless</i>	29
<i>Scan</i>	29
<i>Mac Acl</i>	31
<i>System</i>	32
<i>System</i>	32
<i>System Properties</i>	32
<i>Language</i>	32
<i>Web Server</i>	32
<i>Time Synchronization</i>	33
<i>Logging</i>	33
<i>Password</i>	34
<i>Backup / Upgrade</i>	34
<i>Backup</i>	34
<i>Restore</i>	34
<i>Flash new firmware</i>	35
<i>Reboot</i>	36
<i>Reboot</i>	36
<i>Schedule Reboot</i>	36
<i>System Log</i>	37
<i>Tools</i>	38
<i>Diagnostics</i>	38
<i>Ping Watchdog</i>	39
<i>Device Discovery</i>	40
<i>Alignment</i>	41
<i>Spectrum Analysis</i>	42
<i>Channel Scan</i>	43
<i>Wireless Link Test</i>	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

 STREAM 60GHz Range 49

 Industrial Network Transmission..... 49

 Intelligent Wi-Fi Solutions 49

 Industry Leading Technical Support 49

INTRODUCTION

This User Guide describes the firmware version 2.2.3 20260711 and above which is integrated into all Pro Range G5 products provided by SilverNet Ltd.

SUPPORTED PRODUCTS

This manual covers all GEN5 products listed below:

- MICRO
- LITE
- BASE

For more information, visit www.silvernet.com

WIRELESS MODES

The Pro Range supports the following wireless modes:

- Station WDS
- 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)

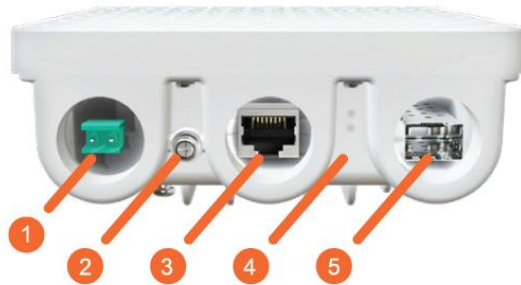
PACKING LIST

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



LED	Description
Ethernet	On: The radio has a wired connection Flashing: Data transferring over the wire
SFP	On: The radio has an SFP connection Flashing: Data transferring over the SFP
75% Signal RX	On: Signal Strength -75dBm to -65dBm
100% Signal RX	On: Signal Strength more than -65dBm

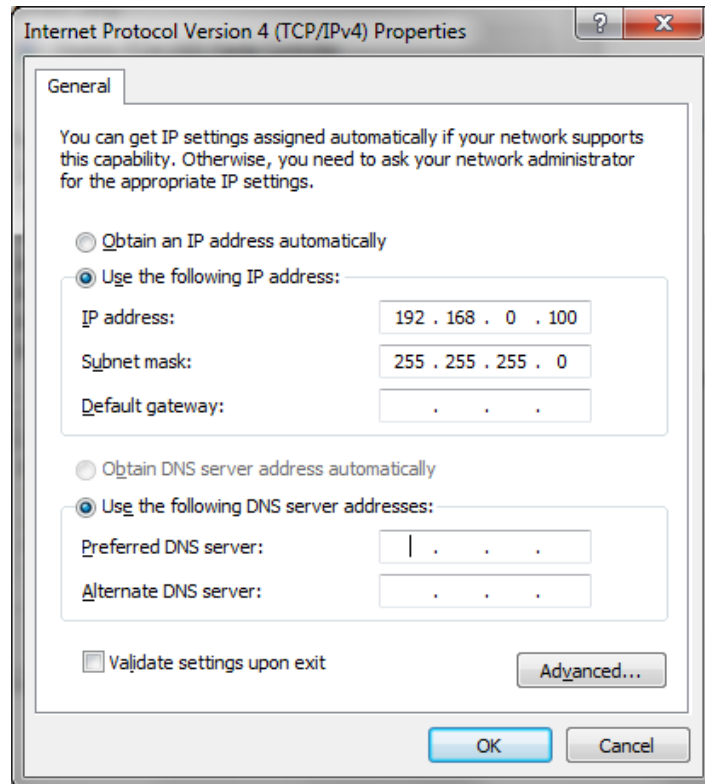
NO	Description
1	DC Port
2	Reset button – Press for 10s to restore to factory settings
3	Ethernet Port
4	Moisture Vent
5	SFP+ Port

CONFIGURATION

GETTING STARTED

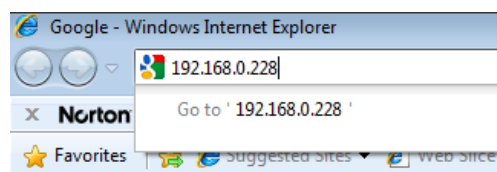
To access the Pro Range Configuration Interface, perform the following steps:

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

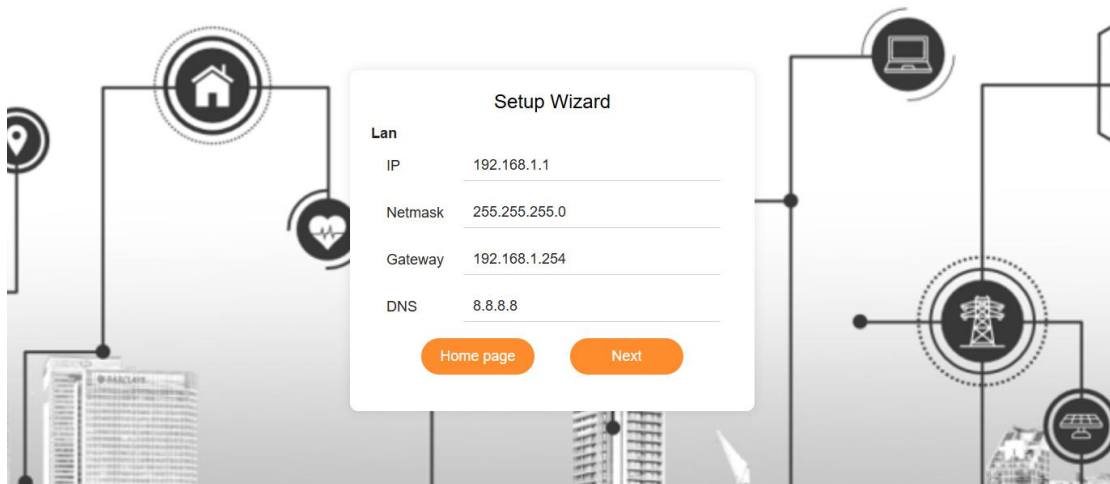


If the unit has been reset, it will go to the default IP address of 192.168.1.1. You will need to change your Ethernet adapter IP address to 192.168.1.x subnet.

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

SETUP WIZARD

If you reset the device it will go to the default IP address of 192.168.1.1. Once you login you will have the option to use the Setup Wizard or skip and go straight to the Home page.



IP 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

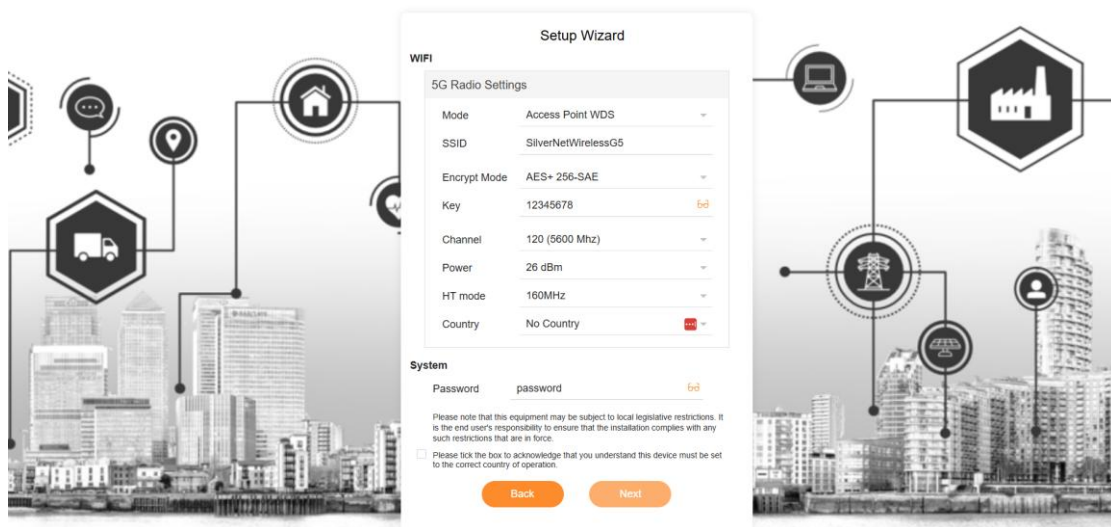
Gateway (optional) Enter the gateway IP address of the network the device is connected to.

DNS (optional) Enter the IP address for the DNS server you wish to use. The default is 8.8.8.8

Home page Allows you to skip the Setup Wizard and go directly to the management interface.

Next Proceed to the next configuration step of the Setup Wizard.

Continue using the wizard to configure the wireless settings.



Mode Select the transmission mode. Access Point WDS (Rx) or Client WDS (Tx) mode.

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

Encryption Select the wireless encryption you wish to use. AES+ 256-SAE is the default.

Key Enter the encryption key you wish to use.

Channel Set the channel number/frequency that the device will use.

Power Set the maximum output power.

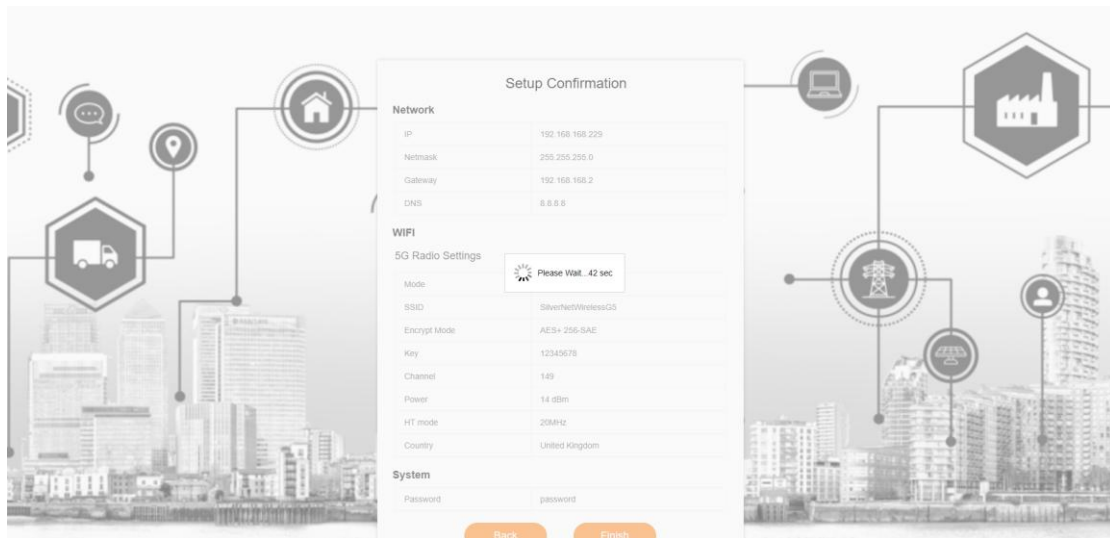
HT Mode High Throughput mode. Select the channel width you want to use.

Country code Select the country of operation.

Password Enter the password you wish to set for the device. Default is password is "password". We recommend you change the password.

Next Proceed to the next configuration step of the Setup Wizard.

Confirm the information is correct.



The image shows a 'Setup Confirmation' screen for a SilverNet wireless network. The screen is divided into three main sections: Network, WIFI, and System. The Network section shows IP, Netmask, Gateway, and DNS. The WIFI section shows 5G Radio Settings, including Mode, SSID, Encrypt Mode, Key, Channel, Power, HT mode, and Country. The System section shows a Password field. At the bottom, there are 'Back' and 'Finish' buttons. A 'Please Wait. 42 sec' message is displayed in the center of the WIFI section.

Setup Confirmation	
Network	
IP	192.168.168.229
Netmask	255.255.255.0
Gateway	192.168.168.2
DNS	8.8.8.8
WIFI	
5G Radio Settings	
Mode	Please Wait. 42 sec
SSID	SilverNetWirelessG5
Encrypt Mode	AES+ 256-SAE
Key	12345678
Channel	149
Power	14 dBm
HT mode	20MHz
Country	United Kingdom
System	
Password	password

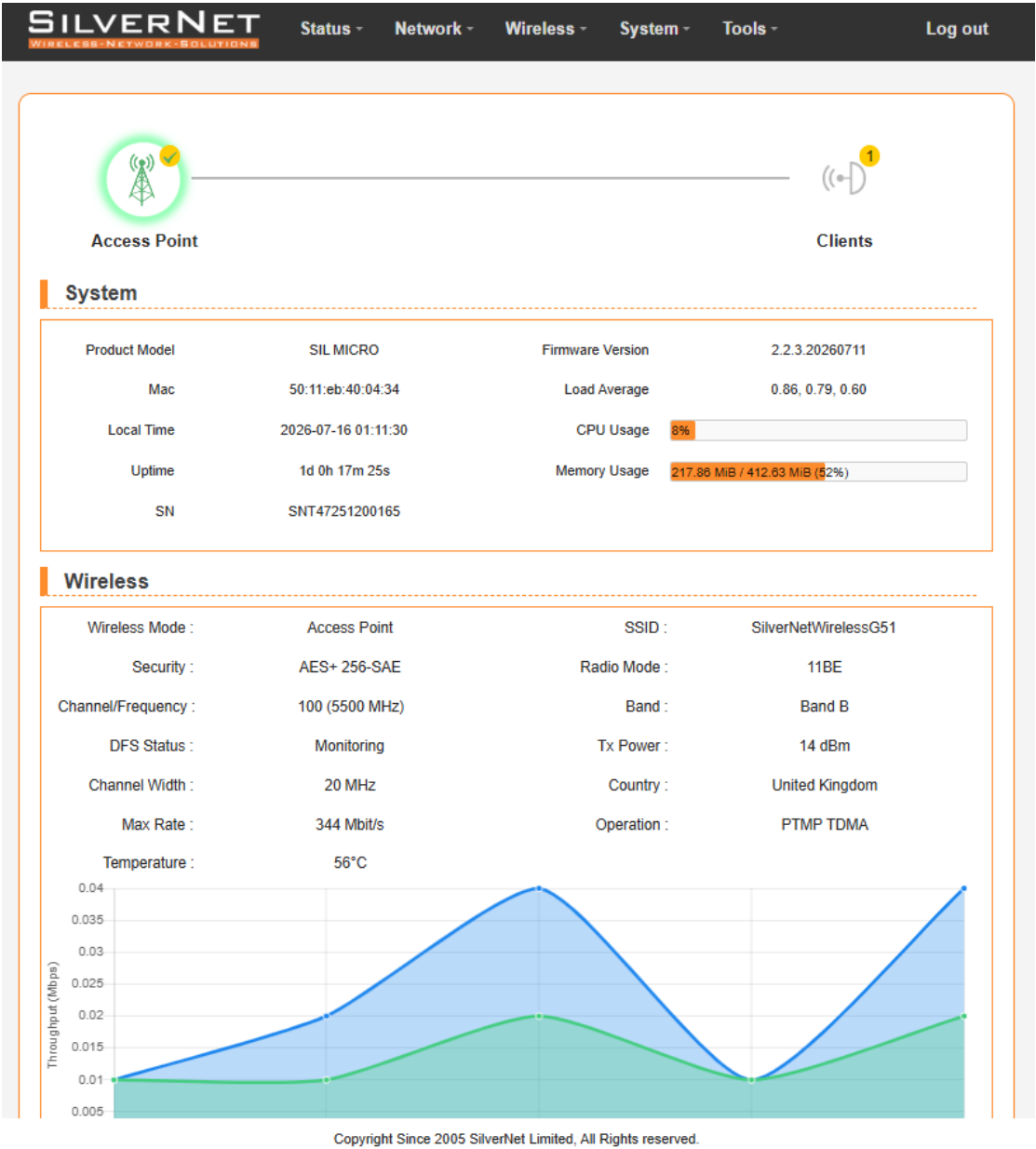
Back Allows you to go back and edit the configuration.

Finish Completes the setup and takes you to the Home page.

STATUS

OVERVIEW

The Status Overview 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.



SYSTEM

Product Model This shows you the model name of the device.

MAC Physical address (MAC Address) used to identify the device on the network.

Local Time Displays local device date and time information. Can be changed in System properties.

Uptime The length of time the device has been continuously running as normal since startup.

SN Serial Number: Unique identifier for each product, used for tracking the production batch and date.

Firmware Version Displays the current version of firmware loaded into the device.

Load Average Measures overall system load, reflecting resource contention (especially CPU, memory, I/O) over a period.

CPU Usage An indicator measuring the current usage of the devices central processor over a period of time.

Memory usage Displays the amount of memory resources currently being used by the system during its operation.

WIRELESS

Wireless Mode This shows you the operating mode of the device. Access Point or Client.

Security Shows the Wireless encryption method. Current supported options: AES+ 256-SAE, AES+ 256 GEN4, AES+ 256 GEN3, AES+ 128 GEN2, OFF.

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

DFS Status Shows the current status of the DFS scan.

Channel Width Shows the channel size/bandwidth occupied by the wireless signal. Currently supported channel widths are: 20MHz, 40MHz, 80MHz, 160MHz.

Max Rate Theoretical maximum data transfer rate of the device. Shown in Mbps.

Temperature Displays the current temperature of the device.

SSID Displays the name of the wireless network.

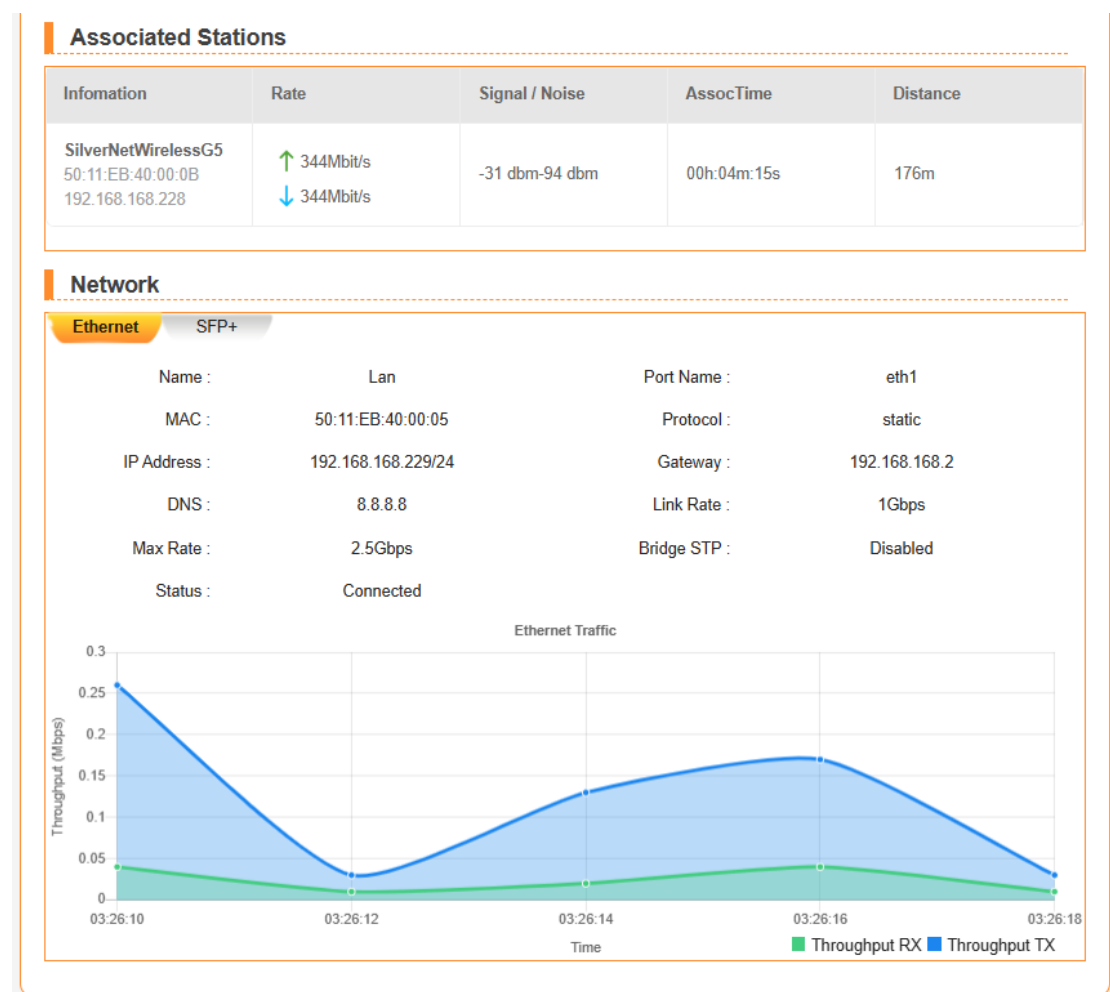
Radio Mode Shows the IEEE 802.11 standard the wireless device is currently operating on.

Band Displays the current operating channel band if an appropriate country code is selected.

Tx Power The current transmit power in dBm used by the device when transmitting.

Country Displays the country code the device has been set to.

Operation Displays the current mode that has been selected. PTP (Point to Point) or PTMP (Point to Multi-Point with Time-Division Multiple Access).



ASSOCIATED STATIONS

Information Displays information about the connected device such as SSID, MAC address and IP address.

Rate Shows the theoretical data transfer rate (in Mbps) between the connected devices.

Signal/Noise Shows the receive signal and the noise levels of the connection.

AssocTime Displays the length of time that the link has been connected/Associated.

Distance Displays the distance between Access Point and the Client.

NETWORK

Name Will show LAN or SFP+ depending on the physical port connected.

MAC Physical address (MAC Address) used to identify the device on the network.

IP address Shows the IP address of the device.

Subnet Mask (/24): Indicates the first 24 bits are the network part, last 8 bits are the host part (Decimal subnet mask: 255.255.255.0).

DNS Shows the current DNS server IP address.

Max Rate Theoretical maximum data transfer rate of the device.

Status Connection status of the eth1/eth0 physical interface.

Port Name Shows the physical interface assigned.

Protocol Shows the Ethernet interface protocol being used.

Gateway Shows the gateway IP address.

Link rate Shows the actual data transfer rate of the Ethernet port connected to the network.

Bridge STP Shows the status of the Spanning Tree function (Enabled/Disabled).

ROUTING

This section allows you to view the IP addresses and MAC addresses of devices connected to the local area network (LAN), as well as the IPv4 routing and forwarding paths currently in use.

ARP (ADDRESS RESOLUTION PROTOCOL)

ARP is a protocol used in IPv4 networks to map an IP address to its corresponding physical MAC address. It enables devices within the LAN to identify each other at the data-link layer, ensuring proper packet delivery on the local network.

ACTIVE IPV4 ROUTES

Routing is the process of forwarding IP packets from a source host to a destination host across one or more networks.

Active Routes represent the routing entries that are currently in effect and used to determine how packets are forwarded. These entries are stored in the device's routing table (i.e., the page you are viewing) and are maintained by network devices such as routers and bridges.

Active IPv4 ARP					
IP address	MAC address	Interface			
192.168.1.102	00:E0:4C:68:00:2C	lan			
192.168.168.228	50:11:EB:40:00:08	lan			
192.168.168.2	00:1D:AA:14:0F:D0	lan			
192.168.168.79	6C:6E:07:02:84:F3	lan			

Active IPv4 Routes					
Network	Target	Gateway	Metric	Table	Protocol
lan	0.0.0.0/0	192.168.168.2	0	main	static
lan	192.168.1.102	-	0	main	
lan	192.168.168.0/24	-	0	main	kernel

NETWORK

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

- **Configuration:** This allows you to set the management port of the device.
- **LAN:** This allows you to configure the IP Address settings, DHCP Server Settings, DNS Settings and Physical settings.
- **VLAN:** This allows you to enable and manage VLANs.

NETWORK

Status ▾
Network ▾
Wireless ▾
System ▾
Tools ▾
Log out

Configuration

Manage Interfaces

ALL ▾

LAN

Protocol

Static address ▾

IPv4 address

192.168.20.120

IPv4 netmask

255.255.255.0 ▾

IPv4 gateway

192.168.20.1

IPv6 address

IPv6 gateway

DNS

8.8.8.8

⊗

⊕

MTU

1500

Enable STP
☐

VLAN

Name	VLAN ID	Untagged Interface	Tagged Interface	IP Address	MAC Address
This section contains no values yet					

Add VLAN

Save & Apply ▾

LAN

Protocol Select the IP protocol you wish to use. Available options are Static address, DHCP Client, DHCPv6 Client.

IPv4 Address Enter the IP address you wish to use. (e.g. 192.168.0.228)

IPv4 Netmask Enter the subnet mask for the IP address. (e.g. 255.255.255.0)

IPv4 Gateway Enter the gateway address. (e.g. 192.168.0.254)

DNS (optional) Enter the IP address for the DNS server you wish to use. The default is 8.8.8.8

MTU Sets the maximum transmission unit (MTU), the default being 1500 bytes, we recommend you do not change this unless you have a good reason to.

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.

VLAN

To create a VLAN, click “Add VLAN”. A window will appear.

Add Vlan configuration

Name
vlan998

VLAN ID
998

Untagged Interface
unspecified

Tagged Interface
ETH1 WLAN

MAC address

Dismiss
Save

Name Enter the name of your VLAN.

VLAN ID Enter the VLAN number you wish to use.

Untagged Interface Select the interface that the VLAN is for.

Tagged Interface Select the interface that the VLAN is for.

MAC address Can be left blank or you can manually enter the MAC address.

Click Save to create the VLAN.

LAN_VLAN998

Protocol

Static address

IPv4 address

IP (x.x.x.x)

IPv4 netmask

255.255.255.0

IPv4 gateway

192.168.20.1 (lan)

IPv6 address

+

IPv6 gateway

VLAN

Name	VLAN ID	Network	Interface	IP Address	MAC Address	
vlan998	998	LAN	ETH1,WLAN	-	-	EditDelete

Add VLAN

Save & Apply

Copyright 2005 - 2025 SilverNet Limited, All Rights reserved.

Once the VLAN is created you can configure the IP settings. Once finished, Save & Apply.

LAN_VLAN

Protocol Select the IP protocol you wish to use. Available options are Static address, DHCP Client, DHCPv6 Client.

IPV4 Address Enter the IP address you wish to use. (e.g. 192.168.0.228)

IPV4 Netmask Enter the subnet mask for the IP address. (e.g. 255.255.255.0)

IPV4 Gateway Enter the gateway address. (e.g. 192.168.0.254)

DNS (optional) Enter the IP address for the DNS server you wish to use. The default is 8.8.8.8

VLAN

Name Shows the name of your VLAN.

VLAN ID Shows the VLAN number.

Interface Shows the interfaces the VLAN is set up on.

IP address Shows the VLAN IP address.

MAC Shows the MAC address of the device.

To make your new VLAN the management VLAN just select it from the drop-down menu and then **Save & Apply**.

Warning: Once this setting is enabled, you must have your management VLAN settings correctly configured or you will not be able to reach your device again without resetting to defaults.

SILVERNET

WIRELESS-NETWORK-SOLUTIONS

Status - Network - Wireless - System - Tools - Log out

Configuration

Manage Interfaces ALL

LAN

Protocol LAN_VLAN998

IPv4 address 192.168.20.120

IPv4 netmask 255.255.255.0

IPv4 gateway 192.168.20.1

IPv6 address

IPv6 gateway

DNS 8.8.8.8

MTU 1500

Enable STP

Note: You may have to reboot the device for the VLANS to take effect.

VLAN

Name	VLAN ID	Network	Interface	IP Address	MAC Address	
vlan998	998	LAN	ETH1,WLAN	-	-	EditDelete

Add VLAN

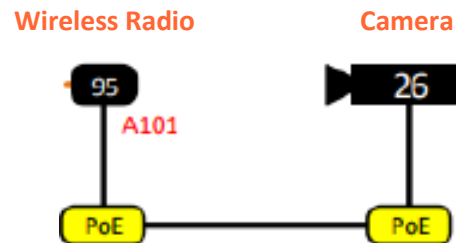
Save & Apply

Copyright 2005 - 2025 SilverNet Limited, All Rights reserved.

To edit a VLAN, click the Edit button. To delete a VLAN, click the Delete button. Once finished, Save & Apply.

Data VLAN

If you need to put a device like a Camera onto a VLAN but do not want to use a switch you can use this method. In this scenario we want our camera to be on VLAN 101



click "Add VLAN". A window will appear.

Add Vlan configuration

Name
vlan101

VLAN ID
101

Untagged Interface
ETH1

Tagged Interface
WLAN

MAC address

Dismiss
Save

Name Enter the name of your VLAN. In this scenario it will be Vlan101.

VLAN ID Enter the VLAN number you wish to use. In this case it will be 101.

Untagged Interface We want to untag the Ethernet interface (ETH1). This means that the traffic with the specified VLAN ID (in this case 101) received over the upstream wireless link will have the VLAN tag removed as it exits the wired ports. Similarly, traffic coming into the device over the wired ports (the Camera) will be tagged with the specified VLAN ID when it's sent over the wireless link.

Tagged Interface We want to tag the wireless interface (WLAN). This means the device keeps the VLAN tag on the Ethernet frame as it leaves the port (or wireless link). The device will expect any traffic coming into it over the port (or wireless link) to already have a VLAN tag and will treat it according to that tag.

MAC address Can be left blank or you can manually enter the MAC address.

Click Save to create the VLAN.

LAN_VLAN101

Protocol

Static address

IPv4 address

IP (x.x.x.x)

IPv4 netmask

255.255.255.0

IPv4 gateway

192.168.20.1 (lan)

IPv6 address

+

IPv6 gateway

VLAN

Name	VLAN ID	Untagged Interface	Tagged Interface	IP Address	MAC Address	
vlan101	101	ETH1	WLAN	-	-	Edit Delete

Add VLAN

Save & Apply

Once the VLAN is created you can configure the IP settings. Once finished, Save & Apply.

LAN_VLAN

Protocol Select the IP protocol you wish to use. Available options are Static address, DHCP Client, DHCPv6 Client.

IPv4 Address Enter the IP address you wish to use. (e.g. 192.168.0.228)

IPv4 Netmask Enter the subnet mask for the IP address. (e.g. 255.255.255.0)

IPv4 Gateway Enter the gateway address. (e.g. 192.168.0.254)

DNS (optional) Enter the IP address for the DNS server you wish to use. The default is 8.8.8.8

Note: You may have to reboot the device for the VLANS to take effect.

TR069

The CPE WAN Management Protocol is a network management protocol that enables service providers (SPs) to remotely manage and configure customer-premises equipment (CPE), such as routers, optical network terminals, and set-top boxes. It is widely used in broadband, IoT, and other deployment scenarios to support large-scale device configuration, monitoring, and maintenance

TR069 Configuration

Enable ☐

ACS URL

ACS Username

ACS Password

Periodic Enable ☐

Periodic Interval

Connect Request

Username

Password

[Save & Apply](#)

Enable Use to turn the protocol on or off.

ACS URL The web address for the remote management server.

ACS Username Username for your CPE to log into the ACS.

ACS Password Password for your CPE to log into the ACS.

Periodic Enable Enable or disable this setting.

Periodic Interval Enter the time (in seconds) between connection requests from CPE to ACS.

Connect Request

Username Username for the ACS to authenticate and connect back to your device.

Password Password for the ACS to authenticate and connect back to your device.

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.

Snmp Setting

Server Enabled ☒

Protocol Version

Server Port

Get Community

Set Community

Location

Contact

Name

[Save & Apply](#)

SNMP V2 Settings

Server Enabled Enable or Disable SNMP

Protocol Version Select the version of SNMP you wish to use.

Server Port Default port number for SNMPv2 “listening” is 161 and “receiving traps” is 162. We recommend you use the default ports and do not change them unless necessary.

Get Community This is the read-only community string. Allows retrieval of device information. Default is public.

Set Community This is the read-write community string. Allows modification of device settings. Default is private.

Location Enter the server’s physical location to assist with network inventory and identification.

Contact Enter the email address of the person responsible for managing the device.

Name Enter the device name or identifier used to distinguish it within your network.

SILVERNET
WIRELESS-NETWORK-SOLUTIONS

Status - Network - Wireless - System - Tools - Log out

Snmp Setting

Server Enabled ☒

Protocol Version SNMPv3

Server Port UDP:161,UDP6:161

User Name

Access Level Read Only

Auth Protocol SHA

Auth Password

Privacy Protocol AES

Privacy Password

Location office

Contact bofh@example.com

Name SilverNet

Save & Apply

Copyright Since 2005 SilverNet Limited, All Rights reserved.

SNMP V3 Settings

Server Enabled Enable or Disable SNMP.

Protocol Version Select the version of SNMP you wish to use.

Server Port Defines the UDP ports used for SNMP communication. The default listening port is 161. These should only be changed if your network configuration requires custom ports.

User Name Specify the SNMPv3 user account that will be used for authenticated access to the device.

Access Level Choose the permission level assigned to the SNMPv3 user. “Read Only” allows viewing device information; “Read Write” permits configuration changes.

Auth Protocol Select the authentication protocol used to verify the SNMPv3 user’s identity. Options are SHA or MD5. SHA is recommended because it provides stronger integrity protection.

Auth Password Enter the password associated with the authentication protocol. This must match the credentials configured on the SNMP manager.

Privacy Protocol Choose the encryption method used to secure SNMP data. Options are AES or DES. AES is recommended as it offers stronger encryption and better security.

Privacy Password Enter the password used for encrypting SNMP messages. This ensures confidentiality of the data exchanged.

Location Enter the physical location of the device to assist with network inventory and identification.

Contact Provide the email address of the person responsible for managing or monitoring the device.

Name Enter the device name or identifier used to distinguish it within your network.

WIRELESS

WIRELESS

The Wireless tab contains everything needed to set up the wireless part of the link.

SILVERNET
WIRELESS-NETWORK-SOLUTIONS

StatusNetworkWirelessSystemTools

Log out

Wireless Configuration

Operation

☒ PTP☐ PTMP TDMA

Mode

Access PointClient

SSID

SilverNetWirelessG5

Encryption

AES+ 256-SAE

Key

6d

Hide SSID

☐

Isolate Clients

☐?

Output Power (EIRP)

22 dBm

Operating frequency

Mode

BE

Band

Band B

Channel

5600(DFS)

Width

160 MHz

Modulation Rate

AUTO

Country

United Kingdom

?

Antenna Gain

16

2.4G Wireless

Wireless network is disabled

Enable

SSID

SilverNet24

Encryption

WPA3-SAE

Key

6d

Save & Apply

Copyright 2005 - 2025 SilverNet Limited, All Rights reserved.

WIRELESS CONFIGURATION

Operation Choose the operation mode. PTP (Point to Point) or PTMP TDMA (Point to Multi-Point with Time-Division Multiple Access).

Mode Select the transmission mode. Access Point (Rx) or Client (Tx) mode. Client mode has a Scan option which will be covered below.

SSID Enter the name of the wireless network that the device should transmit, the Service Set Identifier (SSID), is what you will see if you scan with your laptop.

Encryption Select the wireless encryption you wish to use. AES+ 256-SAE is the default.

Key Enter the encryption key you wish to use.

Hide SSID Once checked, this will disable advertising the SSID of the access point in broadcast messages to wireless stations.

Isolate Clients Prevents Client-to-Client communication.

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

Operating frequency

- **Mode** Select the IEEE 802.11 standard to use. Default is BE
- **Band** Some countries like the UK have Frequency bands. Select the correct frequency band for your country. Band B is the unlicensed outdoor band for EU.
- **Channel** The default, Auto, allows the device to automatically select the channel. 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.
- **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.

Modulation rate Select the modulation rate. When left on **auto** the modulation 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.

Country 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 band, channels and output power will be tuned according to the regulations of the selected country.

ANTENNA GAIN

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. When using a SIL BASE you can set this depending on the antenna you have, e.g. 12dBi Omni or 18dBi Sector. 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.

2.4G WIRELESS

Enable Enable or Disable

SSID Enter the name of the wireless network that the device should transmit, the Service Set Identifier (SSID), is what you will see if you scan with your laptop.

Encryption Select the wireless encryption you wish to use. WPA3-SAE is the default.

Key Enter the encryption key you wish to use.

SCAN

In Client mode you can start a wireless scan. Click the scan button to begin. The radio will then scan the 5GHz band and show any networks it can detect. This will allow you to see any potential interference issues and assist with better network management. You can also connect to one of the networks as long as you have the correct credentials.

Join Network: Wireless Scan

Signal	SSID	Channel	Mode	BSSID	Encryption	
-58 dBm	hidden	149	Master	50:11:EB:30:00:4F	WPA2 PSK (GCMP-256)	Join Network
-67 dBm	SilverNet	64	Master	50:11:EB:11:00:E5	WPA2 PSK (CCMP, GCMP, CCMP-256, GCMP-256)	Join Network
-67 dBm	WirelessNet	64	Master	56:11:EB:11:00:E5	WPA2 PSK (CCMP, GCMP, CCMP-256, GCMP-256)	Join Network
-67 dBm	SilverNetWireless-12	149	Master	50:11:EB:30:00:10	WPA2 PSK (CCMP)	Join Network

To connect to one of the available networks click the “Join Network” button. This will then take you to the config page where you will need to enter the correct security key to connect.

Wireless Configuration

Operation ☒ PTP ☐ PTMP TDMA

Mode

Scan

SSID

Encryption

Key

Once done, click “Save & Apply”.

MAC ACL

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.

Deny List Click Add to add a MAC address to this list.

Allow List Click Add to add a MAC address to this list.

Hostname Give this MAC address a name.

MAC-Address Select the MAC from the dropdown list or enter a custom MAC address.

One you are finished, click Save.

SYSTEM

SYSTEM

SYSTEM PROPERTIES

System Properties

Local Time

2026-01-12 11:53:24

Sync with browser

Hostname

SilverNet

Timezone

(GMT) Greenwich Mean Time

Local Time Displays the device time. After changing the time zone you can sync the time by clicking the Sync with browser button.

HostName Used to identify and distinguish between different devices on the network.

Timezone Use to select the correct time zone.

LANGUAGE

Language and Style

Language

English

Language Default is English. Choose a language from the menu.

WEB SERVER

Web server

Secure Connection (HTTPS)

☐

Secure server port

Server port

80

Secure Connection (HTTPS) Click to enable HTTPS.

Secure server port Port 443 is the default port for HTTPS traffic.

Server port Port 80 is the default port for HTTP traffic.

TIME SYNCHRONIZATION

Time Synchronization

Enable NTP client ☒

Provide NTP server ☐

NTP server candidates

0.time.google.com

1.time.cloudflare.com

Enable NTP client Click to enable NTP Client.

Provide NTP server Click to make the device an NTP server.

NTP Servers Enter the NTP servers you wish to use.

Please note that the device will need internet access for this to work.

LOGGING

Logging

System log buffer size	64
External system log server	0.0.0.0
External system log server port	514
Log output level	Debug
Cron Log Level	Debug

Save & Apply

System log buffer size This defines how much log data the device stores in memory in KB.

External system log server This is the IP address of the remote syslog server. 0.0.0.0 means no external server configured.

External system log server port - Port 514 is the standard syslog port (UDP by default). Leave this unless your syslog server uses a custom port.

Log output level This controls how detailed the logs are.

Cron Log level This controls how much detail is logged from scheduled tasks.

PASSWORD

Password Enter your new administrator password.

Confirmation Confirm your new administrator password.

BACKUP / UPGRADE

BACKUP

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

RESTORE

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.

FLASH NEW FIRMWARE

Image Select the firmware file you wish to upgrade and click upload to begin the update process. Once the file is validated it will ask if you want to keep settings.

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

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

Status -
Network -
Wireless -
System -
Tools -
Log out

Reboot

Reboots the operating system of your device

Perform reboot

Schedule Reboot

Current Time | 2026-01-08 16:56:49

Enable ☐

Time

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

Save & Apply

REBOOT

Reboot Reboots the device.

SCHEDULE REBOOT

Enable Enable or disable scheduled reboot.

Time Select the time you wish the device to reboot.

Week Tick the days of the week to enable the auto reboot.

Click Save & Apply.

SYSTEM LOG

The system log is a collection data that records the operating status, events, and error information generated by the operating system of the device. Good for supporting health monitoring, troubleshooting, operational auditing, and performance optimization.

System Log

Log Type: DEFAULT

Current Time | 2026-01-08 17:01:41

Search...

Refresh Clear All

```
Tue Jan 6 04:30:00 2026 cron.err crond[11769]: USER root pid 4779 cmd /lib/superos/ac/lowi_cpe.sh
Tue Jan 6 04:32:42 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:32:46 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:32:50 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:36:38 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:38:25 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:39:17 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:40:48 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:41:09 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:41:54 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:44:05 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:44:31 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:44:45 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:45:11 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:45:45 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:46:49 2026 daemon.warn dnsmasq[1]: possible DNS-rebind attack detected: requality.android.shouji.sogou.com
Tue Jan 6 04:48:47 2026 daemon.warn dnsmasq[1]: possible DNS-rebind attack detected: requality.android.shouji.sogou.com
Tue Jan 6 04:50:10 2026 daemon.warn dnsmasq[1]: possible DNS-rebind attack detected: requality.android.shouji.sogou.com
Tue Jan 6 04:50:25 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:53:43 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:54:15 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:54:23 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:54:36 2026 daemon.warn odhcpd[11474]: No default route present, overriding ra_lifetime!
Tue Jan 6 04:55:50 2026 daemon.warn dnsmasq[1]: possible DNS-rebind attack detected: requality.android.shouji.sogou.com
Tue Jan 6 04:57:42 2026 daemon.warn dnsmasq[1]: possible DNS-rebind attack detected: requality.android.shouji.sogou.com
```

1 2 3 4 5 ... 27

Log Type Select the system log type, the system supports log type filtering: DEFAULT, DEBUG, INFO, NOTICE, WARNING, ERROR, CRIT, ALERT, EMERG.

Search Can be used to search for specific information.

TOOLS

DIAGNOSTICS

The screenshot shows the SilverNet Network Utilities interface. At the top, there is a navigation bar with the SilverNet logo and links for Status, Network, Wireless, System, Tools, and Log out. Below the navigation bar, the 'Network Utilities' section is active. It contains three input fields for IP addresses and three buttons: 'IPv4 Ping', 'IPv4 Traceroute', and 'Nslookup'. The 'IPv4 Ping' button is selected, and the results of the ping test are displayed in a text area. The results show a successful ping to 192.168.168.228 with 5 data bytes, 5 packets transmitted, and 5 packets received, resulting in 0% packet loss. The round-trip times are 2.624, 3.205, and 4.676 ms.

```

PING 192.168.168.228 (192.168.168.228): 56 data bytes
64 bytes from 192.168.168.228: seq=0 ttl=64 time=2.757 ms
64 bytes from 192.168.168.228: seq=1 ttl=64 time=3.278 ms
64 bytes from 192.168.168.228: seq=2 ttl=64 time=2.693 ms
64 bytes from 192.168.168.228: seq=3 ttl=64 time=2.624 ms
64 bytes from 192.168.168.228: seq=4 ttl=64 time=4.676 ms

--- 192.168.168.228 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.624/3.205/4.676 ms
  
```

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.

PING WATCHDOG

Generally used on the Client end to ping the AP and reboot itself if it cannot get a response.

Ping WatchDog

Enable ☐

Enable ping watchdog to reboot this device when it is unable to ping the specified IP address.

IP Address to Ping

Startup Delay (s)

Ping Interval (s)

Failure count

Ping fail action

Save & Apply

Enable Enable or disable Ping Watchdog.

IP address to Ping Enter the IP address for the device to ping.

Startup Delay Set the length of time in seconds the device will wait before starting the ping requests. We would recommend a minimum of 120 seconds to give the device time to boot up and try to establish a link. If using on the AP end then we recommend a minimum of 720 seconds to allow for DFS scans.

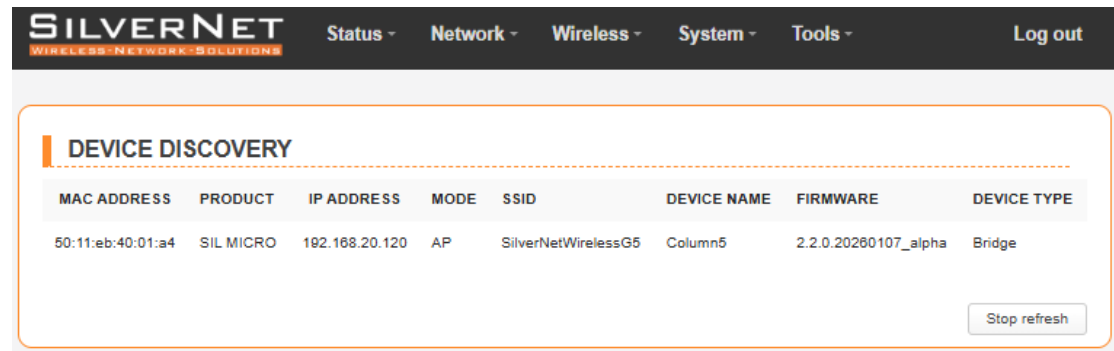
Ping Interval How often the ping will be sent (in seconds). For example, every 10 seconds.

Failure Count The number of missed pings before the device applies the ping fail action.

Ping fail action Select the action the device will take when the pings are missed. Reboot Wireless will just restart the wireless interface. Reboot Radio will reboot the entire device.

DEVICE DISCOVERY

This will show any SilverNet Gen5 devices connected to the same network.



MAC ADDRESS	PRODUCT	IP ADDRESS	MODE	SSID	DEVICE NAME	FIRMWARE	DEVICE TYPE
50:11:eb:40:01:a4	SIL MICRO	192.168.20.120	AP	SilverNetWirelessG5	Column5	2.2.0.20260107_alpha	Bridge

Stop refresh

MAC Address Displays the MAC address of the device.

Product Displays the product type, MICRO, LITE or BASE.

IP Address Displays the IP address of the device.

Mode Shows you what mode the device is set to.

SSID Displays the SSID of the device.

Device Name Displays the name of the device.

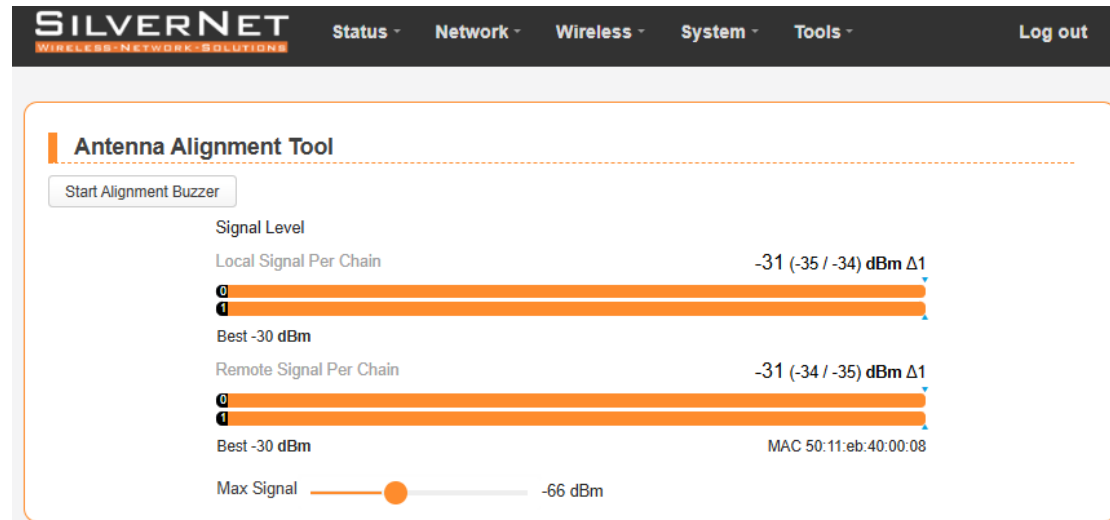
Firmware Shows the current firmware version on the device.

Device Type Displays the device type.

You can stop and start the discovery scan by clicking Stop refresh or Start refresh.

ALIGNMENT

Shows local and remote signal levels that can be used for alignment. By adjusting the direction or elevation angle of the device you may improve signal strength of the link.



Start Alignment Buzzer Click this to start the alignment buzzer. The faster the buzzer sound the stronger the link. Click again to stop.

Local signal per chain Shows the receive signal of your local device. Signal is displays in dBm. The closer to 0 the better the signal. A good signal varies depending on the environment but usually anything between -30 to -45 is considered a good signal. Anything -65 or more is considered a poor link. The (Δ) indicates the difference in signal strength between the two chains.

Best Shows the best signal you have achieved. Useful for alignment.

Remote signal per chain Shows the receive signal of your Remote device. Signal is displays in dBm. The closer to 0 the better the signal. A good signal varies depending on the environment but usually anything between -35 to -45 is considered a good signal. Anything -65 or more is considered a poor link. The (Δ) indicates the difference in signal strength between the two chains.

Best Shows the best signal you have achieved. Useful for alignment.

MAC Shows the MAC address of the remote device.

Max Signal Sets the reference point for the signal level indicator bars. When the actual signal strength reaches this value, the signal bars will show as full. For example, if Max Signal is -66 dBm and the current signal strength is -65 dBm, the signal bars will be completely filled.

SPECTRUM ANALYSIS

This scan can be used to help identify potential interference issues in the current environment.

Status ▾
Network ▾
Wireless ▾
System ▾
Tools ▾
Log out

Spectrum Analysis

Note: Use this scan to analyse the selected spectrum and help identify potential interference issues in the current environment. Please note that the link will drop when the scan tool is operating.

Start Scan :

Stop Scan :

Show scan history :

Start Scan Click to start the scan. Wait while the scan begins to initialise.

Start Scan : Scanning...,Waiting for waterfall and waveform charts to be displayed...64sec

Once complete the scan will show the noise peaks over a certain time. Use the key to establish which areas have some noise. For example, below we can see that there is some noise in Band A and some noise in Band C (5745 to 5825) but Band B (5500 to 5700) looks clear.



Stop Scan Stops the scanning process.

Show Scan History Will show the last scan results.

CHANNEL SCAN

The Channel Scan provides a real-time assessment of the 5 GHz wireless environment surrounding the device. It identifies nearby access points, measures signal strength, evaluates background noise, and determines channel utilisation. This information helps installers and network engineers select the optimal operating channel for reliable performance.

[Status](#)
[Network](#)
[Wireless](#)
[System](#)
[Tools](#)
[Log out](#)

Channel Scan Report

Note: Use this scan to analyze the wireless channel environment. Please note that the network connection will be temporarily interrupted while the scan tool is operating.

Start Scan :

Show scan history :

CHANNEL	ACCESS POINTS	MIN RSSI	MAX RSSI	NOISE FLOOR	CHANNEL LOAD
5180(36)	0	-95 dBm	-95 dBm	-96 dBm	0%
5200(40)	0	-95 dBm	-95 dBm	-95 dBm	0%
5220(44)	0	-95 dBm	-95 dBm	-95 dBm	0%
5240(48)	2	-53 dBm	-53 dBm	-95 dBm	1%
5260(52)	0	-95 dBm	-95 dBm	-94 dBm	0%
5280(56)	0	-95 dBm	-95 dBm	-94 dBm	0%
5300(60)	0	-95 dBm	-95 dBm	-94 dBm	0%

Copyright Since 2005 SilverNet Limited, All Rights reserved.

Start Scan Click to start the scan. Wait while the scan begins to initialise.

Show Scan History Will show the last scan results.

Channel Indicates the 5 GHz channel being analysed, shown with its centre frequency.

Access Points The number of external wireless access points detected operating on that channel.

MIN/MAX RSSI The minimum and maximum received signal strength (RSSI) of detected access points.

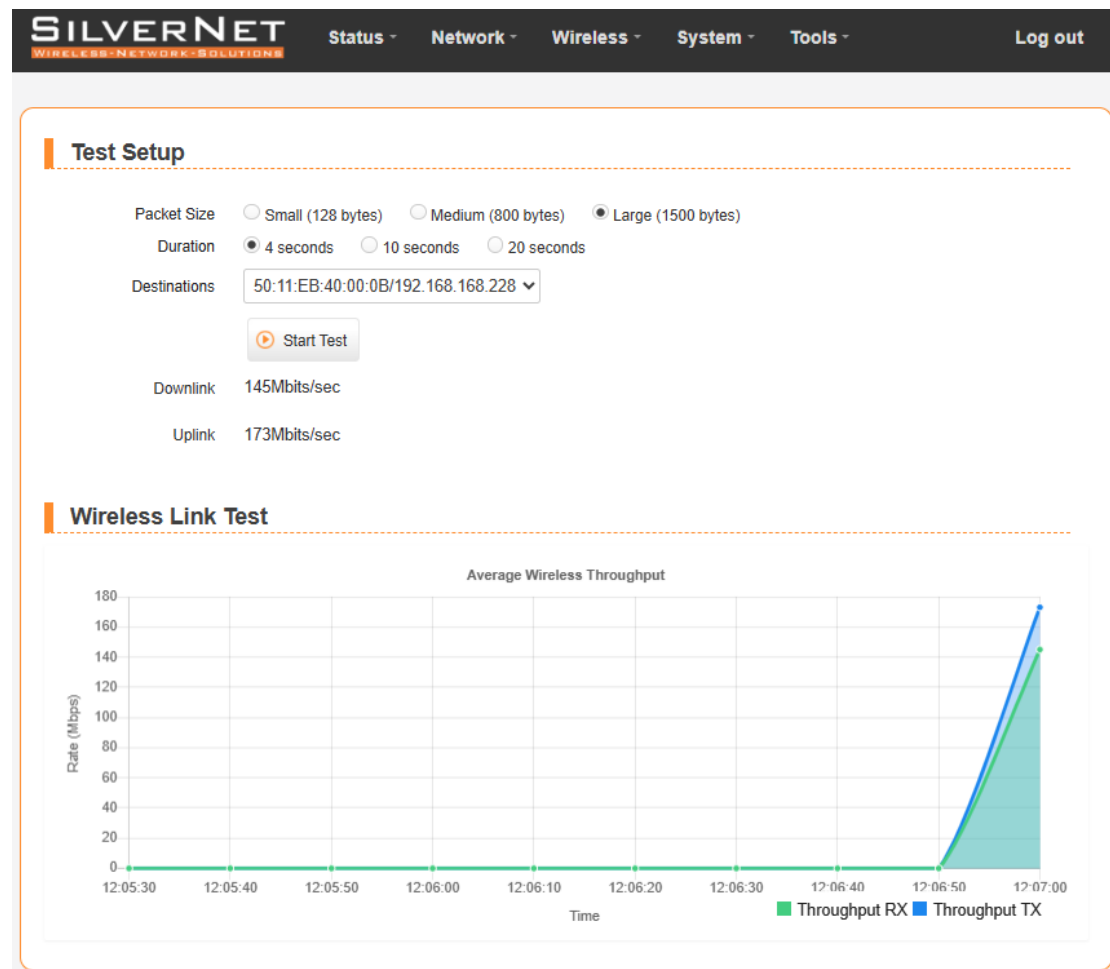
- Values near -95 dBm indicate no meaningful signals present.
- Higher values (e.g., -53 dBm) indicate strong nearby access points.

Noise Floor Represents the background RF noise level on the channel. Typical values around -94 to -96 dBm indicate a clean RF environment.

Channel Load Shows how busy the channel is, expressed as a percentage. Low values (0–1%) indicate minimal utilisation and low interference.

WIRELESS LINK TEST

The wireless link test can be used to test your wireless connection.



Packet Size Select the packet size for the test. We recommend to test with Large packets.

Duration Select the duration of the test. We recommend 20 seconds.

Destinations Select the device to test to using the drop down menu.

Start Test Click start test to speed test the wireless link.

Downlink/Uplink These will be displayed once the test is complete.

Graph Will be displayed once the test is complete.

STANDARDS

DECLARATION OF CONFORMITY

SilverNet Limited declares the following:

Product Name: PRO Range GEN5

Model No.: MICRO, LITE, BASE 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 GEN5 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 licence; the licence is not hard to obtain and is only (at the time of writing) £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 GEN5 comes with a 2-year warranty as standard. For full terms and conditions of warranty please go to www.silvernet.com/terms-and-conditions/

CONTACT SILVERNET

Email us at support@silvernet.com

Call our support team on **08712233067**

www.silvernet.com

COPYRIGHT INFORMATION

Copyright ©2026 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

STREAM 60GHz RANGE



STREAM YOUR WORLD

Industry Leading 60 Ghz Wireless Links

Up to 2KM range
2.5Gbps Throughput
256 AES+

STREAM

INDUSTRIAL NETWORK TRANSMISSION



5 years Warranty

10k bytes Packet

12-56V DC Redundant Power

35°C Operating Temp

IP-40 Enclosure

DIN rail or Wall-mounted Installation

6KV Lightning Protection

SILVERNET

INTELLIGENT WI-FI SOLUTIONS



Intelligent WiFi... **EVOLVED**

Aero
Intelligent Wi-Fi

INDUSTRY LEADING TECHNICAL SUPPORT



Direct Telephone
Technical Support

FAQ

Support

Help

Remote & Onsite
Support when you need it

Training & Support
SILVERNET