48-Port Gigabit Ethernet Web-Managed Switch with 4 SFP Ports

User Manual

Model 561334

INTELLINET®

NETWORK SOLUTIONS

INT-561334-UM-0421-2

1 TABLE OF CONTENTS

2 Product Introduction 4
2.1 Product Overview 4
2.2 Features 4
2.3 Specifications 5
2.4 External Component Description 6
2.4.1 Front Panel 6
2.4.2 Rear Panel 8
2.5 Package Contents 8
3 Installing and Connecting the Switch 9
3.1 Desktop Installation 9
3.2 Rack-mountable Installation in 19-inch Cabinet 9
3.3 Power on the Switch 10
4 Connection to the Switch 11
4.1 Connecting Computer 11
4.2 How to Log in to the Switch 11
5 Saving the Configuration 13
6 Switch Configuration 14
6.1 Home 14
6.1.1 CPU and Memory Status Information 14
6.1.2 Port Information 14
6.2 Quick Setup 16
6.3 Port Settings 17
6.3.1 Basic Config 17
6.3.2 Port Aggregation 19
6.3.3 Port Mirroring 20
6.3.4 Port speed limit 21
6.3.5 Broadcast storm 22
6.3.6 Port isolation 23
6.4 VLAN 26
6.4.1 Trunk Port Settings 28
6.4.2 Hybrid Port Settings 29
6.4.3 Setup Example 30
6.5 Fault/Safety 33
6.5.1 Anti Attack 33
6.5.2 Channel Detection 40
6.5.3 ACL Access Control List 42
6.6 Spanning Tree Protocol (STP) 45
6.6.1 MSTP Region 48
6.6.2 MSTP Bridge 49
6.7 DHCP Relay Agent 51

6.7.1 DHCP Relay 51
6.7.2 Option82 51
6.8 DHCP Server 53
6.8.1 DHCP Config 53
6.9 Terminal Access Controller Access-Control System (TACACS+) 56
6.10 Radius 58
6.10.1 Radius General Config 58
6.10.2 Radius Server Config 59
6.11 AAA 60
6.11.1 Enable Config 60
6.11.2 Region Config 60
6.11.3 Server Config 61
6.11.4 AAA Authentication 62
6.12 QoS – Quality of Service 64
6.12.1 QoS Rules 64
6.12.2 Queue Config 65
6.12.3 Queue Mapping 66
6.13 Address Table 67
6.13.1 Address Table Config 67
6.14 SNMP 69
6.14.1 SNMP Config 69
6.14.2 RMON Config 74
6.15 System 78
6.15.1 System Config 78
6.15.2 System Update 82
6.15.3 Configuration Management 83
6.15.4 Config Save 84
6.15.5 User Accounts 84
6.15.6 Information Collect 85
7 Warranty 86
8 Copyright 87
9 Federal Communication Commission Interference Statement 88

2 PRODUCT INTRODUCTION

Congratulations on your purchase of the Intellinet 48-Port Web-Managed Gigabit Ethernet Switch. Before you install and use this product, read this manual carefully for a full understanding of its functions.

2.1 PRODUCT OVERVIEW

The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch with 4 SFP Ports provides seamless network connections. It integrates 1000 Mbps Gigabit Ethernet, 100Mbps Fast Ethernet and 10Mbps Ethernet network capabilities in a highly flexible package. Each of the 48 10/100/1000 Mbps Auto-Negotiation RJ45 ports support Auto MDI/MDIX function. The switch is a high-performance upgrade from your old network to a 1000 Mbps Gigabit network. It is essential in solving network bottlenecks that frequently develop as more advanced computer users and newer applications demand greater network resources. For efficient management, the switch is equipped with a remote Web interface. The switch can be programmed for advanced management functions such as Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control, MAC Address Table, Diagnostics, RMON and more.

2.2 FEATURES

- Forty-eight 10/100/1000 Mbps auto-sensing ports automatically detect optimal network speeds
- Four small form-factor pluggable GBIC module slots (SFP)
- Complies with the IEEE 802.3az (Energy Efficient Ethernet EEE) specification
- Supports SNMP management
- Supports VLAN (tag-based and port-based)
- Provides IEEE 802.1x port-based security
- Supports link aggregation (trunking)
- Supports port mirroring
- Supports jumbo frames up to 9 kBytes
- Supports Rapid Spanning Tree/Spanning Tree protocol
- Broadcast storm control with multicast packet rate settings
- Supports two types of QoS: port-based and DSCP
- LEDs for power, link/activity, connection speed
- Fanless design ideal for silent operation
- Includes 19" rackmount brackets

2.3 SPECIFICATIONS

Standards

- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.1p (Traffic Prioritization)
- IEEE 802.1q (VLAN Tagging)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3ab (Twisted Pair Gigabit Ethernet)
- IEEE 802.3ad (Link Aggregation Control Protocol LACP)
- IEEE 802.3az (Energy Efficient Ethernet EEE)
- IEEE 802.3u (100Base-TX Fast Ethernet)
- IEEE 802.3x (flow control, for full duplex mode)

Power

- Input: 100 – 240 VAC, 50 – 60 Hz

Environmental

- Metal housing
- Dimensions: 335 (L) x 440 (W) x 44 (H) [mm] (13.19 (L) x 17.32 (W) x 1.73 (H) [in])
- Weight: 4.2 kg (9.26 lbs.)
- Operating temperature: 0 – 40°C (32 – 104°F)
- Operating humidity: 10 – 90% RH, non-condensing
- Storage temperature: -20 – 70°C (-4 – 158°F)

Package Contents

- 48-Port Gigabit Ethernet Web-Managed Switch with Four SFP Ports
- Power cable
- User manual
- 19" rackmount brackets

2.4 External Component Description

2.4.1 Front Panel

The front panel of the switch consists of 48 10/100/1000 Mbps RJ-45 ports, four SFP ports, one Console port, one Reset button and a series of LED indicators as shown below.

10/100/1000 Mbps RJ-45 ports (1~48):

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000 Mbps. Each has a corresponding 10/100/1000 Mbps LED.

SFP ports (SFP1, SFP2, SFP3, SFP4):

Designed to install the SFP module and connect to the device with a bandwidth of 1000 Mbps. All ports have a corresponding 1000 Mbps LED.

Console port (Console):

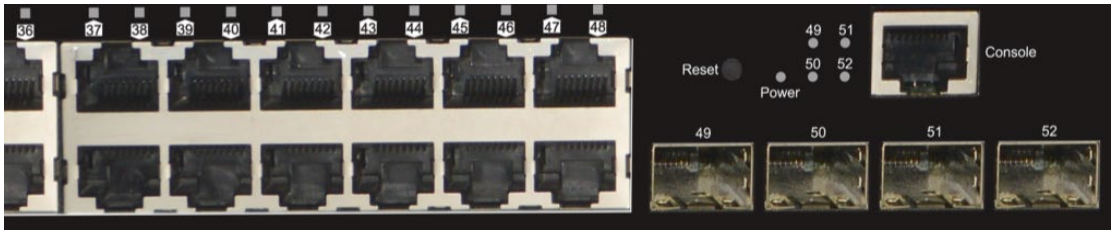
Designed to connect with the serial port of a computer or terminal for monitoring and configuring the switch.

Reset button (Reset):

To restore the system factory default settings, press the reset button for five seconds while the device is powered on.

LED indicators:

The LED indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the switch, its connection or attached devices.



The following chart shows the LED indicators of the switch along with explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
Power	Red	On	Power On
		Off	Power Off
LINK/ACT/ Speed (1~48)	10/100 Mbps: Amber	On	A device is connected to the port
		Off	No device is connected to the port
	1000 Mbps: Green		
		Flashing	Sending or receiving data
SFP1 SFP2 SFP3 SFP4	Green	On	A device is connected to the port
		Off	No device is connected to the port
		Flashing	Sending or receiving data
Reset			Press for 15 seconds – 20 seconds in order to reset all settings to factory default values. Release the button, once the LEDs start flashing.

2.4.2 Rear Panel

AC Power Connector:

Power is supplied through an external AC power adapter. It supports AC 100-240V, 50/60Hz.

Grounding Terminal:

Ground the switch through the PE cable on the AC cord or with a separate ground wire.

2.5 PACKAGE CONTENTS

Before installing the switch, make sure that the following items are enclosed. If any part is missing or damaged, contact your Intellinet agent immediately.

- 48-Port Gigabit Ethernet Web-Managed Switch with 4 SFP Ports
- Power cable
- Quick Installation Guide
- User manual (on CD)
- Four rubber feet, two mounting ears and eights screws

3 Installing and Connecting the Switch

This chapter describes how to install your Web-Managed Gigabit Ethernet Switch and make connections to it. The following steps will help prevent damage to the device and maintain proper security:

- Place the switch on a stable surface or desktop to minimize the chances of it falling.
- Make sure the switch works in the proper AC input range and matches the voltage labeled on the switch.
- To prevent electrocution, do not open the switch's chassis, even if it fails to receive power.
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch.
- Make sure the surface on which the switch is placed can support the weight of the switch and its accessories.

3.1 Desktop Installation

When installing the switch on a desktop (if not in a rack), attach the enclosed rubber feet to the bottom corners of it to minimize vibration. Allow adequate space for ventilation between the device and the objects around it.

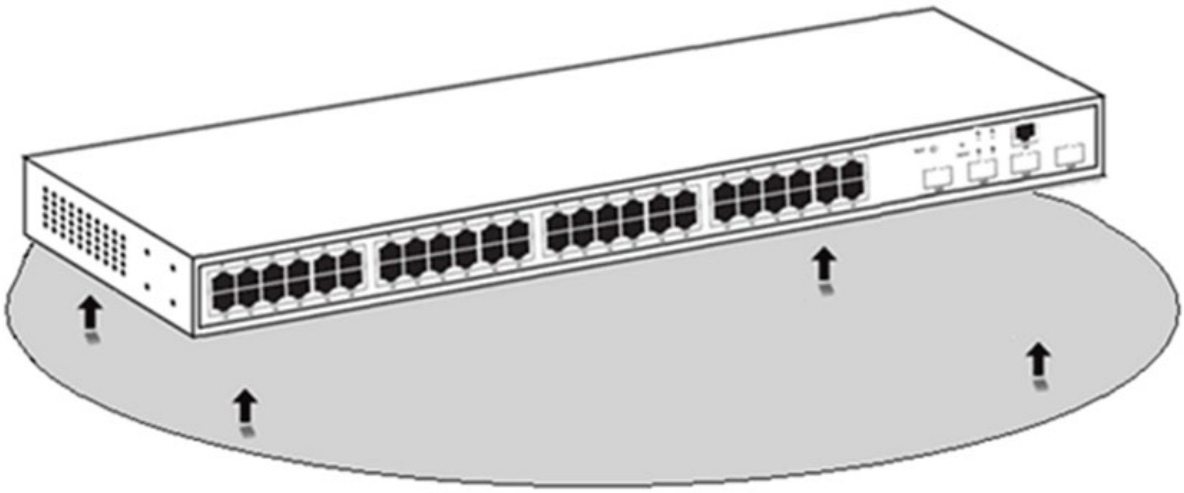


Figure 4 - Desktop Installation

3.2 Rack-mountable Installation in 19-inch Cabinet

The switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the switch, follow these steps:

Attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.

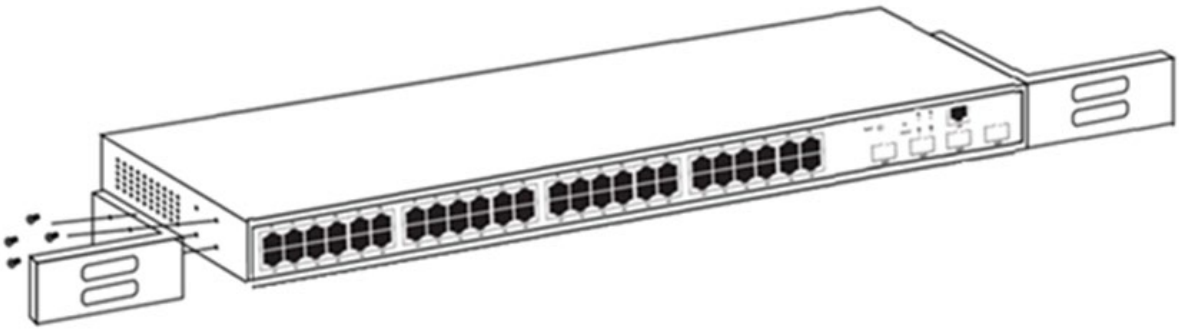


Figure 5 - Bracket Installation

Use the screws provided with the equipment rack to mount the switch on the rack and tighten it.

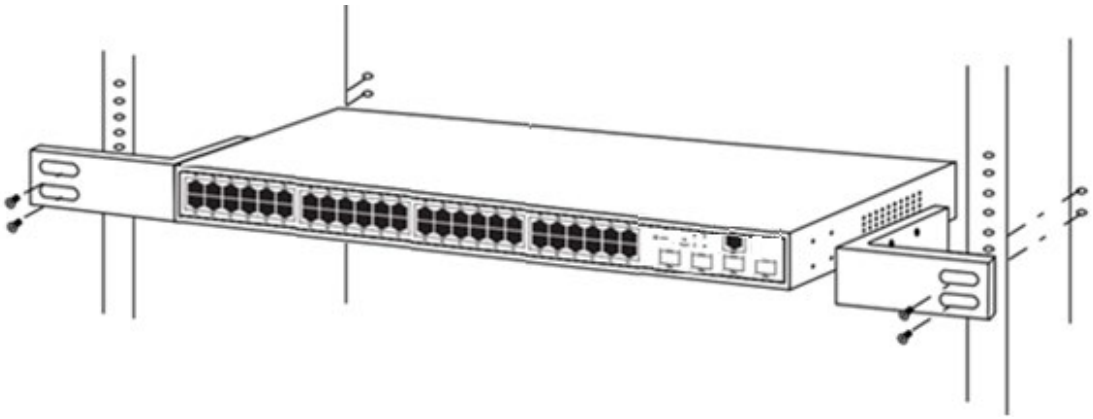


Figure 6 - Rack Installation

3.3 Power on the Switch

The switch is powered on by connecting it to an outlet using the AC 100-240V 50/60Hz internal high-performance power supply.

AC Electrical Outlet:

It is recommended to use a single-phase, three-wire receptacle with a neutral outlet or multifunctional professional receptacle. Be sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:

Connect the AC power connector on the back panel of the switch to an external receptacle with the included power cord, then check that the power indicator is ON. When it is ON, the corresponding LED is illuminated.

4 Connection to the Switch

4.1 Connecting Computer

Use standard Cat5/5e Ethernet cables (UTP/STP) to connect the switch to end nodes as described below. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which they are connected.

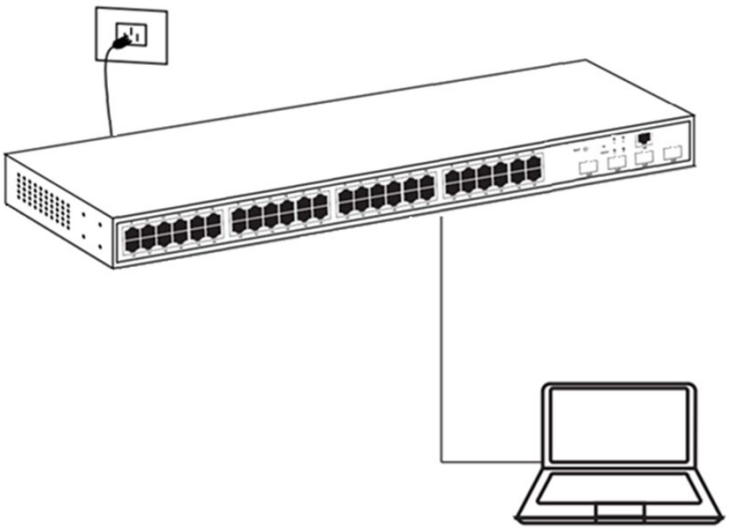


Figure 7 - PC Connect

The LNK/ACT/Speed LEDs for each port are illuminated when the link is available.

4.2 How to Log in to the Switch

As the switch provides Web-based management login, configure your computer's IP address manually to log on to the switch. The default settings of the switch are shown below.

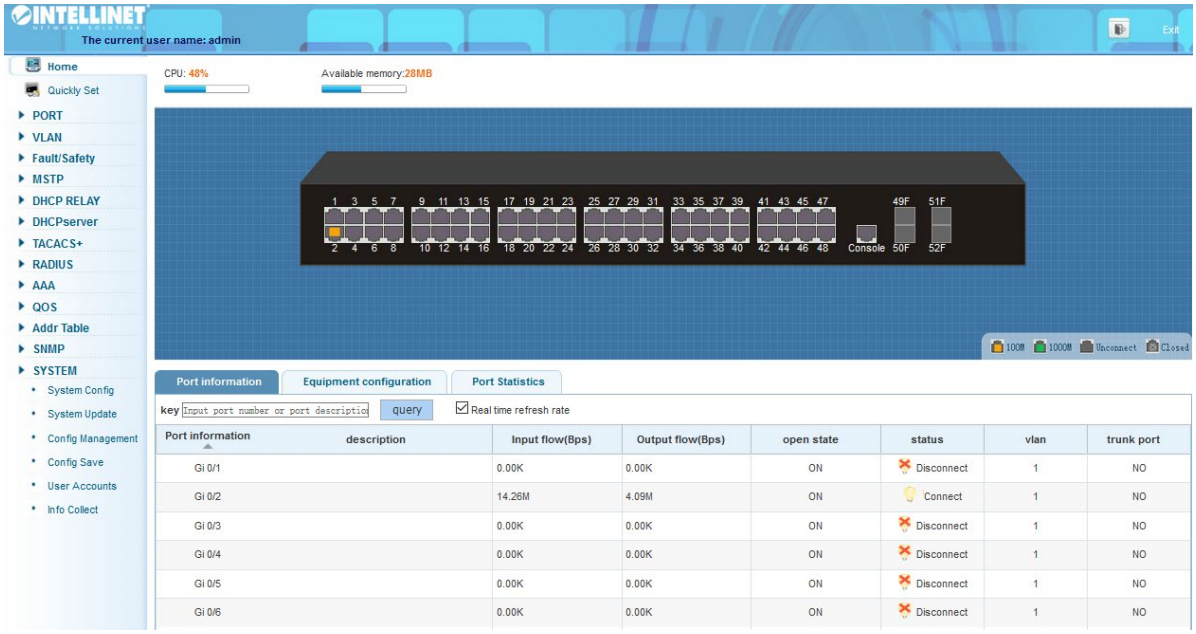
Parameter	Default Value
Default IP address	192.168.2.1
Default Username	admin
Default Password	1234 (or the device serial number)

Log on to the configuration window of the switch through following steps:

1. Connect the switch with the computer NIC interface.
2. Power on the switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" range is 2-254); for example, 192.168.2.100.
4. Note: The default password is either "1234", or the serial number found on the bottom of the device. All later model switches (2020 onwards) use the serial number as the password.

Open the browser, and go to the URL *http://192.168.2.1.* The switch login window appears, as shown below.

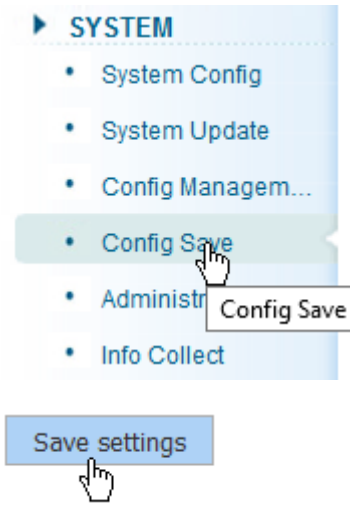
Enter the Username and Password (the factory default Username is **admin** and the Password is **1234** or the **device serial number**), and then click "LOGIN" to log in to the switch configuration window as below.

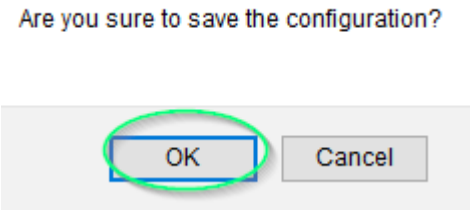


5 SAVING THE CONFIGURATION

The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch provides a myriad of configuration options, many of which are designed for experienced network administrators and aren't easy to configure. It would be a real shame if all the configuration data was lost after a power failure or after the switch was restarted. In order to make the configuration permanent, it needs to be saved.

Here is how:





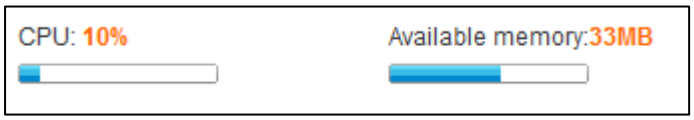
If you do not perform this function, you risk losing all the settings after the switch restarts.

6 SWITCH CONFIGURATION

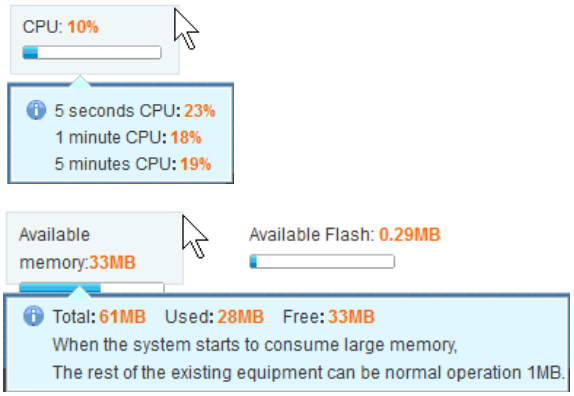
This chapter describes how to use the web-based management interface (Web UI) for this switch.

6.1 HOME

6.1.1 CPU and Memory Status Information

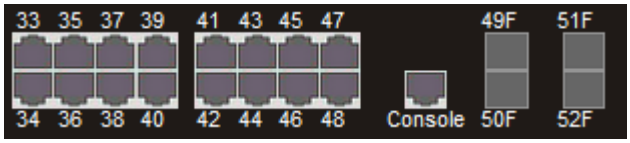


This section provides a quick overview of the switch's basic system resources in terms of memory utilization and CPU load. If you mouse-over any of these sections, additional details are revealed.



If the CPU load is unusually high, or if the available memory or Flash memory is getting low, you may need to restart the Intellinet switch to free up system resources. Initiate the reboot via the SYSTEM -> SYSTEM CONFIG -> SYSTEM RESTART menu.

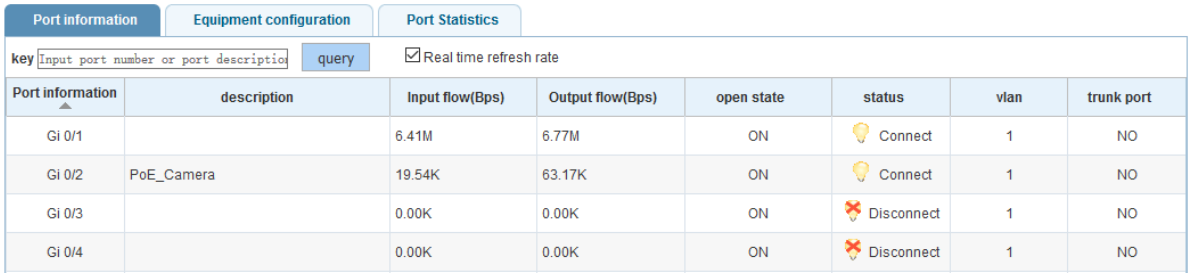
6.1.2 Port Information



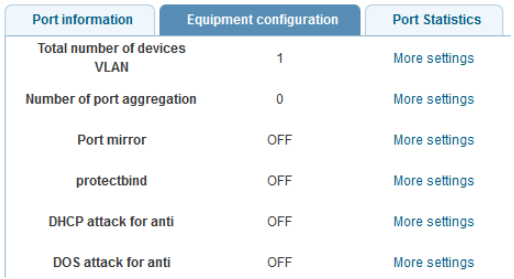
A green squares indicate the port link is up at Gigabit speeds. An amber square indicates a link speed of 100 Mbps. A gray squares indicate the port link is down.

6.1.2.1 *Port Information, Equipment Configuration and Port Statistics*

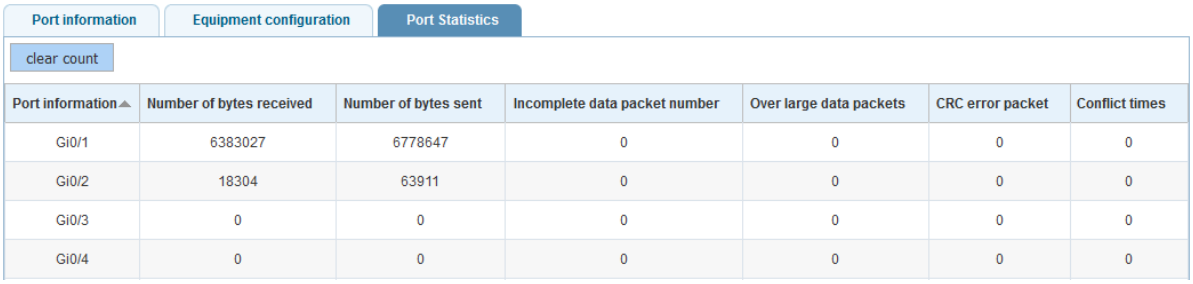
This section provides real-time information about the ports, basic settings and traffic statistics.



Item	Description
Port Information	Displays the port number. The nomenclature is as follows: Gi = Gigabit Ethernet 0/ = Switch 0 (which means this device) 1-52 = Port number. Ports 49, 50, 51 and 52 are SFP module slots.
Description	Optional description for the port, as entered in the basic port configuration.
Input Flow (bps)	Inbound traffic rate, measured in "bits per second."
Output Flow (bps)	Outbound traffic rate, measured in "bits per second."
Open State	ON = Port is activated in the basic port configuration and will accept connections from networking devices. OFF = Port is deactivated in basic port configuration.
Status	Connect: A networking device is connected to the port and has an active link. Disconnect: No device is connected to the port.
VLAN	If the port belongs to a VLAN, its ID is displayed here. ID 1 = default.
Trunk Port	Yes = The port is part of an LACP trunking group. No = The port is not part of an LACP trunking group.



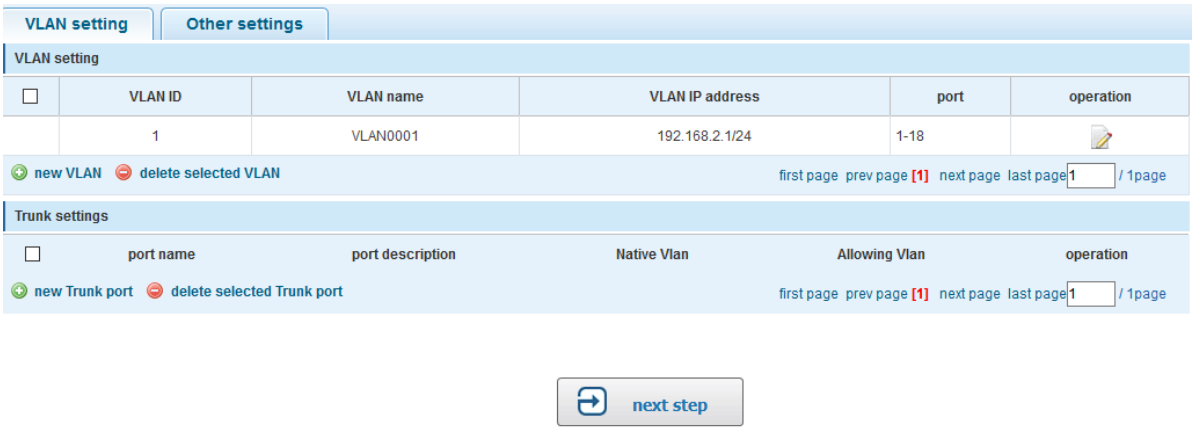
This tab displays information about various functions and provides a short-cut that allows direct configuration of that part of the switch settings.

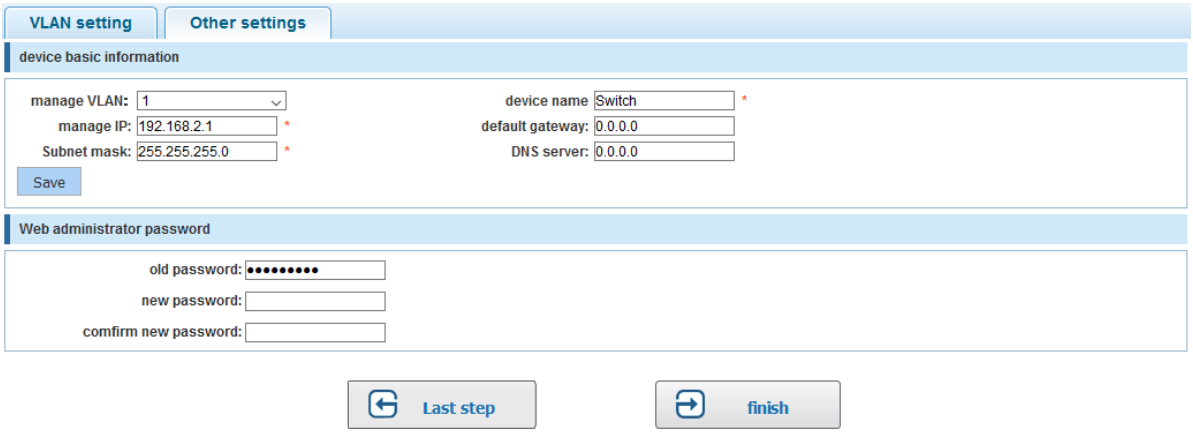


This tab displays real-time information about the data packets for each port.

6.2 Quick Setup

The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch provides a setting that offers direct access to some of the core functions of the device, namely VLAN, trunking, device IP address and admin password. Even though the function is called “Quickly Set,” there is no need to rush. Take as much time as you like with the configuration.



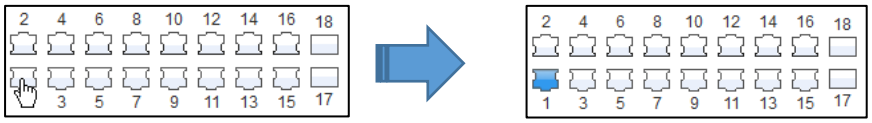


Refer to subsequent sections in this user guide for additional information about the individual functions.

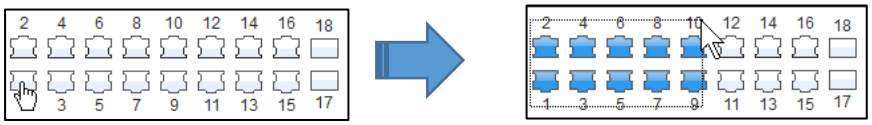
6.3 PORT SETTINGS

6.3.1 Basic Config

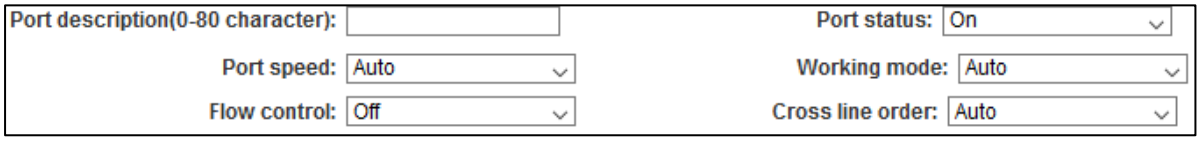
Access the parameters related to each of the 18 ports. The screen is divided into two sections. The upper section displays an image of the 18 ports of the Intellinet switch. In order to make changes to a port, simply click to select it.



Create a selection of multiple ports at once:



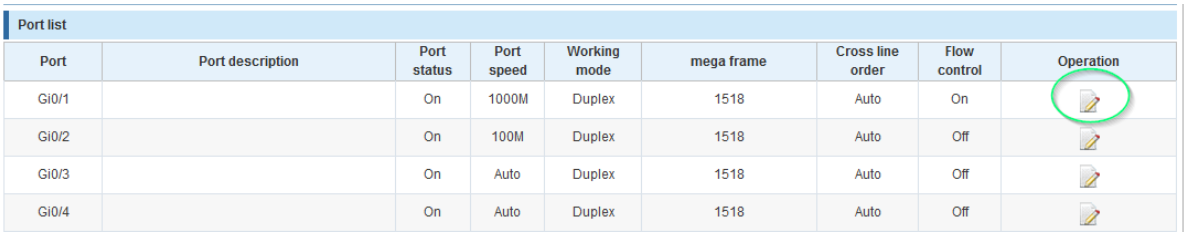
Once one port or multiple ports are selected, make changes to the port settings.



Item	Description
Port description	Optional description for the port. A maximum of 80 characters can be provided. No special characters or spaces are allowed.
Port speed	10M: Force a connection to be made at 10 Mbps. 100M: Force a connection to be made at 100 Mbps. 1000M: Force a connection to be made at 1000 Mbps. Auto: The switch and connected device negotiate the best possible connection speed.
Flow control	IEEE 802.3x flow control is the process of managing the rate of data transmission between two nodes (i.e., the switch and a connected network client) to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from the transmitting node. That sounds like it is a good thing, and it is. So why is the option by default set to “disabled"? The short answer is because you normally don’t need it and because it can, in very rare instances, have a negative impact on the overall performance in your network. The TCP protocol already provides its own flow control mechanism, allowing a sender to throttle back the speed if the receiver is having problems keeping up.
Port status	ON: Activate the port. OFF: Disables the port. No connections to it can be made.

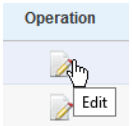
Item	Description
Working mode	This parameter controls the duplex mode. In a full-duplex system, both parties can communicate to the other simultaneously. An example of a full-duplex device is a telephone; the parties at both ends of a call can speak and be heard by the other party simultaneously. In networking terms, full duplex allows receiving and transmitting of data at the same time, whereas half duplex does not. If the telephone is an example for full duplex, then a push-to-talk CB radio or "walkie-talkie" represents half duplex. The switch can either receive or send data, but it can never happen simultaneously. Unless you have a specific reason not to do so, this should be left in “Auto” mode.
Cross line order	Auto MDI-X automatically detects the required cable-connection type and configures the connection appropriately, removing the need for crossover cables to interconnect switches or for connecting PCs peer-to-peer. As long as it is enabled on either end of a link, either type of cable can be used. For auto MDI-X to operate correctly, the data rate on the interface and duplex setting must be set to "auto." When two auto MDI-X ports are connected together, which is normal for modern products, the algorithm resolution time is typically < 500 ms. However, a ~1.4 second asynchronous timer is used to resolve the extremely rare case (with a probability of less than 1 in 5×10^{21}) of a loop where each end keeps switching. If you don’t understand any of this, simply leave this value on “Auto.”

The screen also shows a table that lists all 18 ports along with their parameters. The “mega frame” value refers to jumbo frames, which are Ethernet frames with more than 1500 bytes of payload. Define the size of the jumbo frames in the section SYSTEM -> SYSTEM CONFIG.



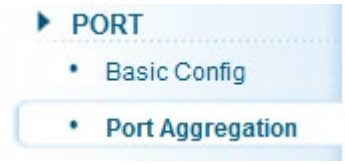
Port list

Port	Port description	Port status	Port speed	Working mode	mega frame	Cross line order	Flow control	Operation
Gi0/1		On	1000M	Duplex	1518	Auto	On	
Gi0/2		On	100M	Duplex	1518	Auto	Off	
Gi0/3		On	Auto	Duplex	1518	Auto	Off	
Gi0/4		On	Auto	Duplex	1518	Auto	Off	

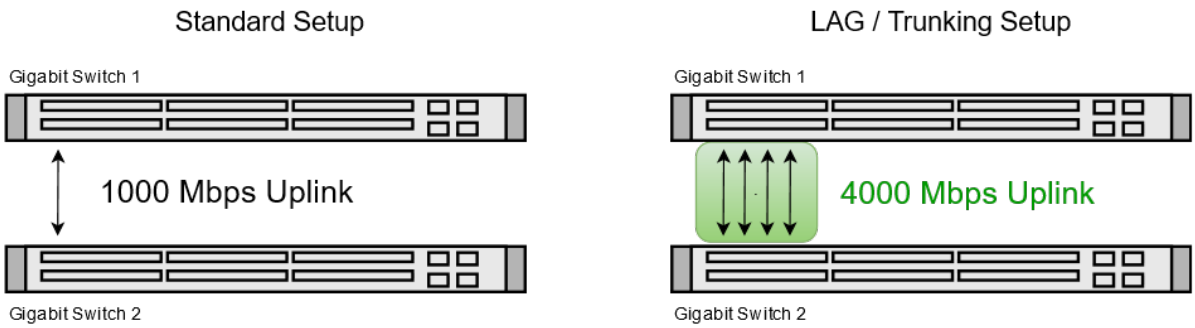


Clicking the pencil allows editing the port settings, exactly the same way as directly selecting the port(s) as shown on the previous page.

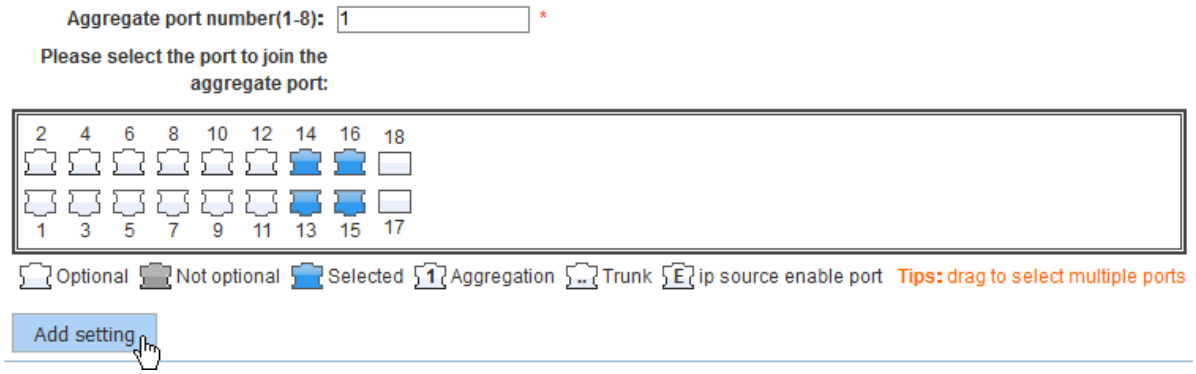
6.3.2 *Port Aggregation*



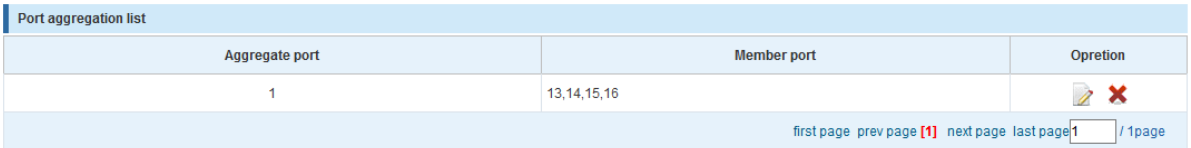
Port aggregation is a method of using multiple Ethernet ports in parallel to increase throughput beyond what a single connection could sustain and to provide redundancy in case one of the links should fail. As this is essentially a grouping of ports into one logical unit, we call them Link Aggregation Groups, or "LAG" for short.



This page is used to set up LAGs. Create up to eight different LAGs; each can have up to eight member ports. Each LAG can be given a custom name, and you must select the ports for the LAG. The example below shows an LAG group set up with four member ports.

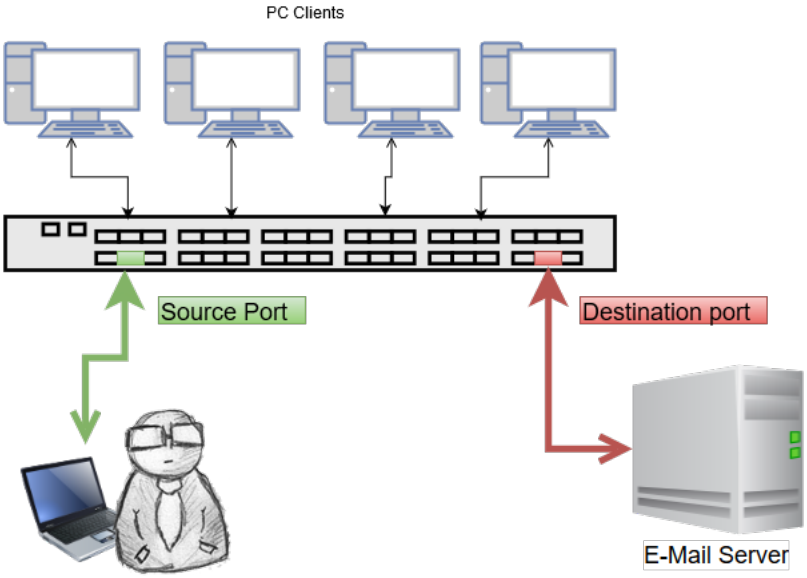


Item	Description
Aggregate port number	This is the link aggregation group (LAG) number
Please select the port to join the aggregate port	Select the member ports that belong to this LAG

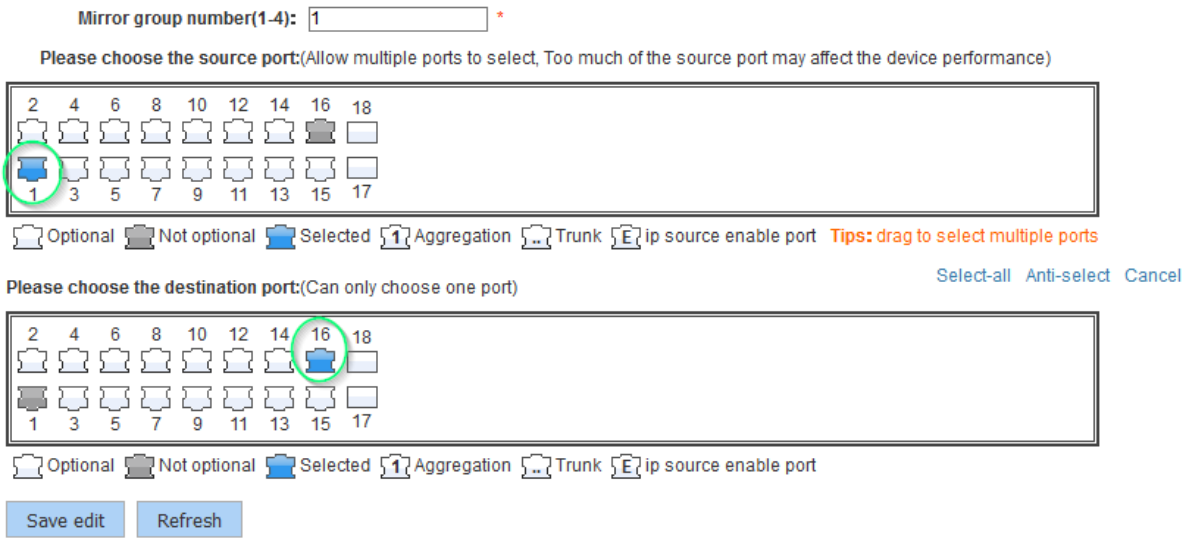


6.3.3 Port Mirroring

Port mirroring is the ability of a network switch to send a copy of network packets seen on a switch port or ports to a network-monitoring device connected to another switch port (i.e., a computer equipped with a packet sniffer utility). The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch provides up to four groups for port-mirroring settings.



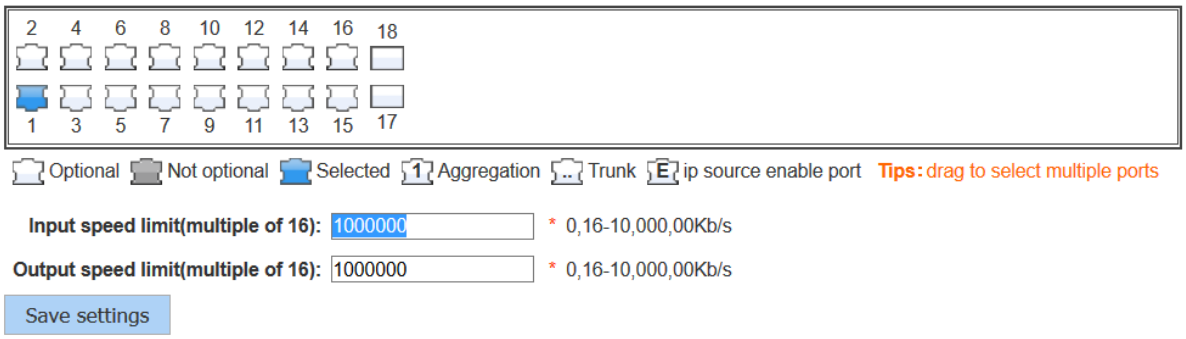
The example below shows setting up one mirror group where all traffic occurring on port 1 is being mirrored to port 16.



6.3.4 *Port speed limit*

This feature allows you to limit the data rates for a particular port on the Intellinet 48-Port Gigabit Ethernet Web-Managed Switch. When the data rate exceeds user-configured values, the Intellinet switch drops packets immediately. Rate limiting is configured for two types of transmissions, which are ingress and egress. Ingress traffic is received on any given port (incoming, inbound, download or input speed), whereas egress traffic is traffic sent out (outgoing, outbound, upload or output speed) to another network client.

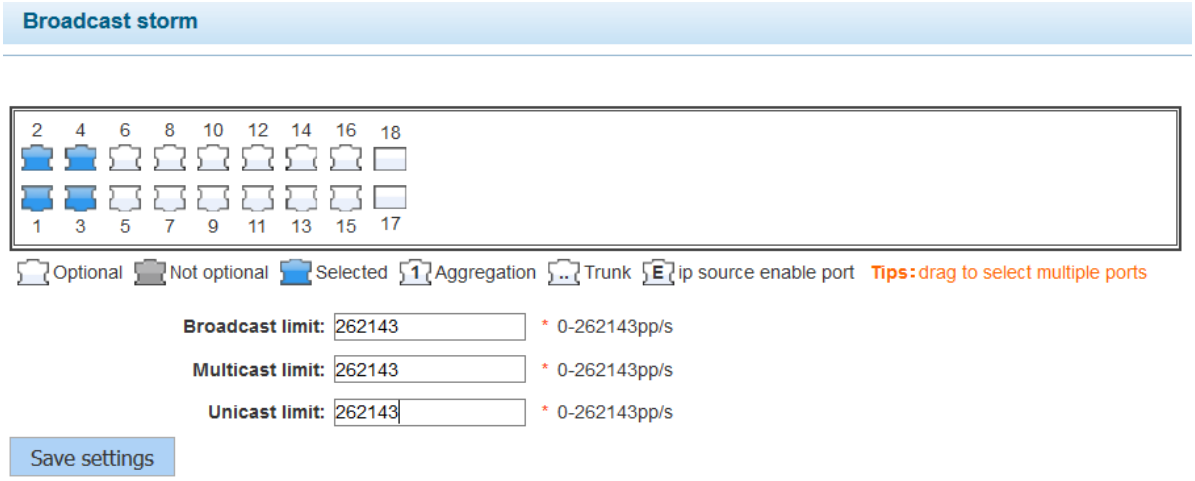
The Intellinet switch allows controlling the available bandwidth for each port individually. The speed is measured in kbps, which stands for kilobits per second. The default is 1 million, which is the equivalent of 1 Gigabit per second. Values entered must be multiples of "16" (e.g., 16, 32, 48, …, 512, …., 1024, etc.).



Item	Description
Port number 1 - 18	Select individual ports or a range of ports.
Input speed limit (multiple of 16)	Provide the ingress rate in kbps.
Output speed limit (multiple of 16)	Provide the egress rate in kbps.

6.3.5 Broadcast storm

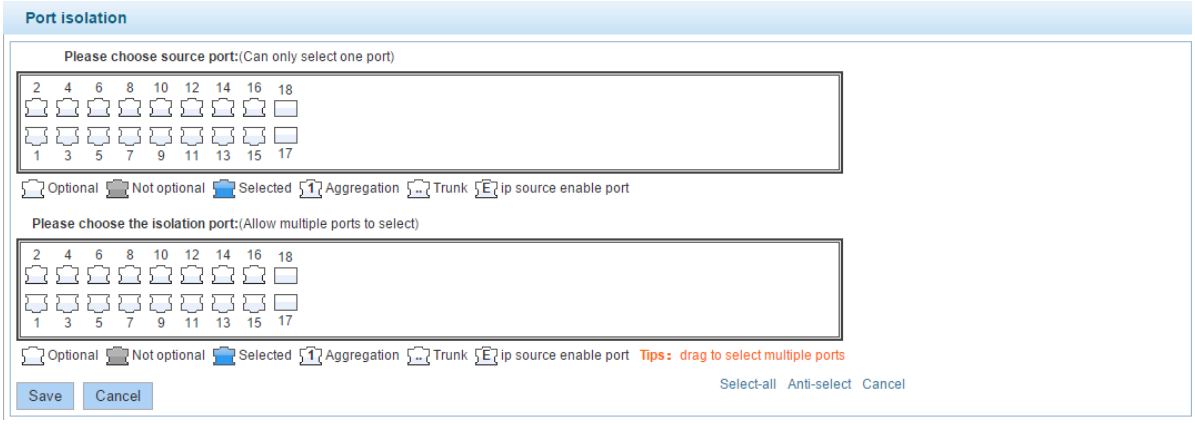
Storm control prevents LAN interfaces from being disrupted by a broadcast storm. A broadcast storm occurs when broadcast packets flood the subnet, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a broadcast storm. The Intellinet switch allows configuring maximum allowed pps rates for three different types of packets. It's possible to set all 18 ports to the same value or provide individual values.



Item	Description
Port number 1 - 52	Select individual ports or a range of ports.
Broadcast limit	Enter the maximum pps (packets per second) for broadcast packets.
Multicast limit	Enter the maximum pps (packets per second) for multicast packets.
Unicast limit	Enter the maximum pps (packets per second) for unicast packets.

6.3.6 Port isolation

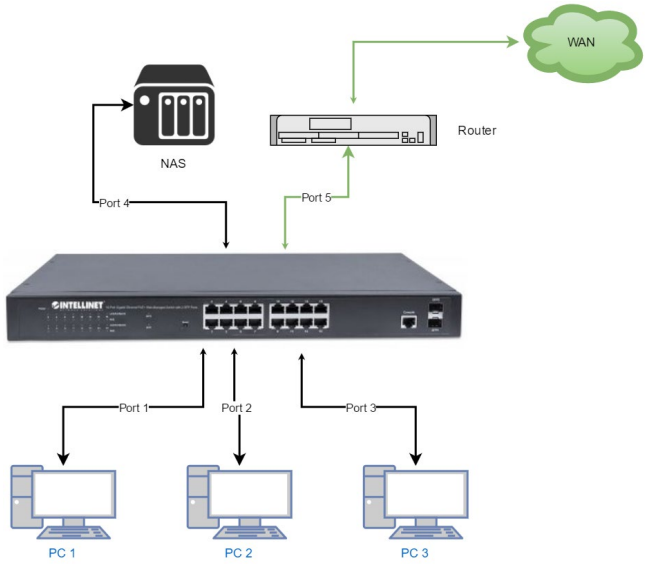
The port isolation function allows you to configure the Intellinet switch in a way, that prevents PCs on different ports from communicating with each other, and all that without configuring a VLAN.



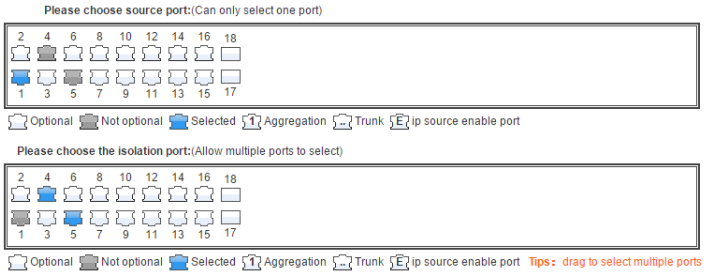
Item	Description
Source Port	Select the port you wish to isolate.
Isolation Port	Select the port(s) to which packets from the source port can be forwarded. More than one port can be selected here.

6.3.6.1 *Configuration Example:*

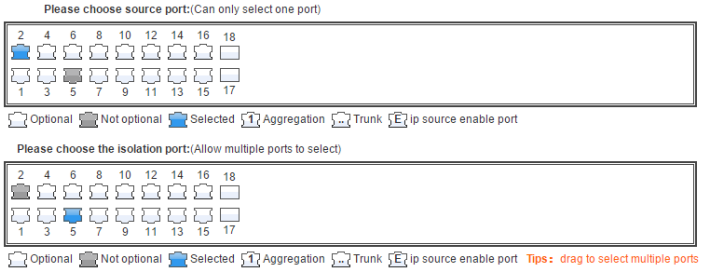
1. Three PCs, one NAS, and one router are connected to the Intellinet switch
2. PC1 is connected to Port 1
3. PC2 is connected to Port 2
4. PC3 is connected to Port 3
5. The NAS is connected to Port 4
6. The router is connected to Port 5
7. PC1 can access the NAS and the router
8. PC2 and PC3 can only access the router



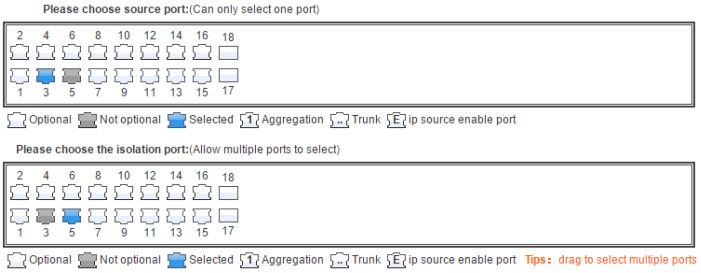
PC1 on port 1:



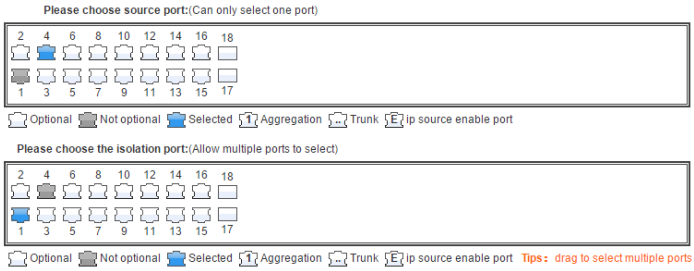
PC2 on port 2:



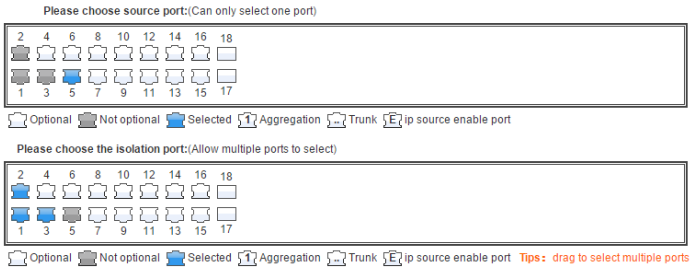
PC3 on port 3:



NAS on Port 4:



Router on Port 5:



When completed, the configuration will look like this. To better understand what is happening, it helps to consider the isolated ports as the ports with which the source ports can communicate.

Port isolation list

Source port	Isolate port	Operation
1	4 5	✖
2	5	✖
3	5	✖
4	1	✖
5	1 2 3	✖

first page prev page [1] next page last page 1 / 1page

6.4 VLAN

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the datalink layer (OSI layer 2). VLANs are datalink layer (OSI layer 2) constructs, analogous to IP subnets, which are network-layer (OSI layer 3) constructs. VLANs can be used to partition a local network into several distinctive segments.

VLAN technology provides the following advantages:

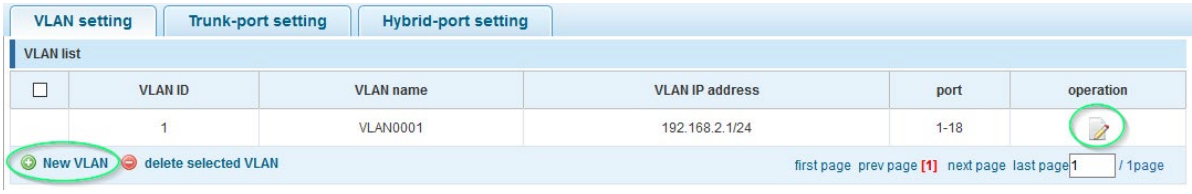
1. Broadcast traffic does not cross into different VLANs, which reduces bandwidth utilization and improves network performance.
2. Security in your LAN can be improved, since packets in different VLANs cannot communicate with each other directly.
3. With VLAN, clients can be allocated to different working groups, and users from the same group do not have to be within the same physical area, which makes network maintenance much easier and more flexible.

VLAN technology knows three types of ports—access, trunk and hybrid ports.

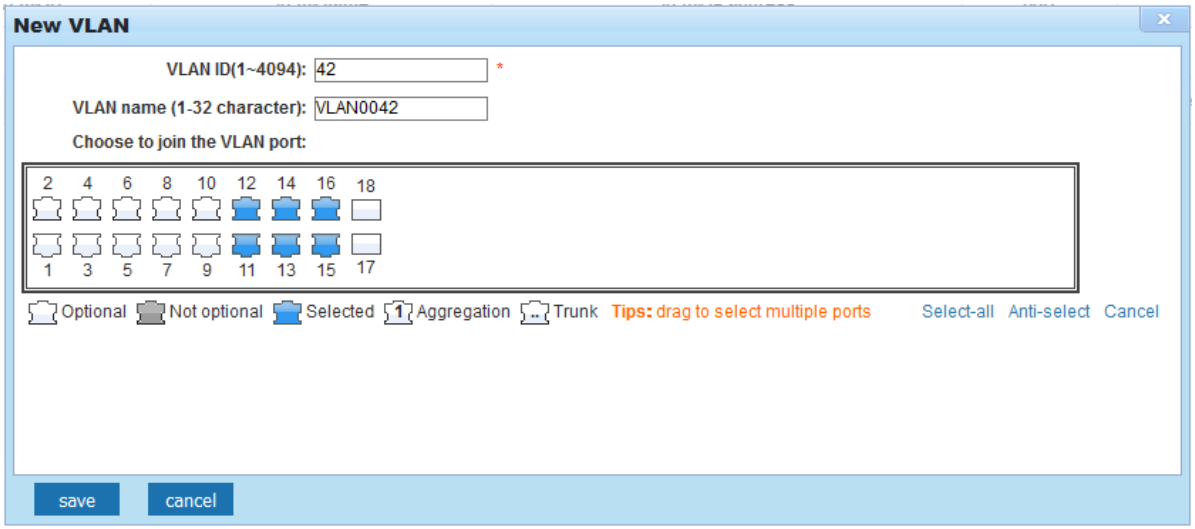
1. Access Ports (untagged)
    a. Access ports are designed to tag any incoming packet with the VLAN ID the port has been assigned to.
    b. Tagged VLAN packets arriving at the access port are dropped by the switch.
    c. As far as the Intellinet switch is concerned, any port that isn't defined as a trunk or hybrid port is considered an access port.

2. Trunk Ports (tagged)
    a. Trunk ports are designed to filter out packets that have either no VLAN tag or VLAN tags that are not on the allowed VLAN ID list.
    b. Trunk ports do not remove any existing VLAN tags from incoming packets.
    c. Trunk ports do not add a VLAN tag to any incoming untagged packet.
    d. Trunk ports are ideal for switch-to-switch connections or for devices that have the ability to tag packets by themselves such as VoIP phones.

3. Hybrid Ports
    a. These are a combination of access and trunk ports.
    b. Hybrid ports will tag any incoming packet that has no VLAN ID with the VLAN ID the port has been assigned to.
    c. Hybrid ports will also act as trunk ports for packets that have a VLAN tag.

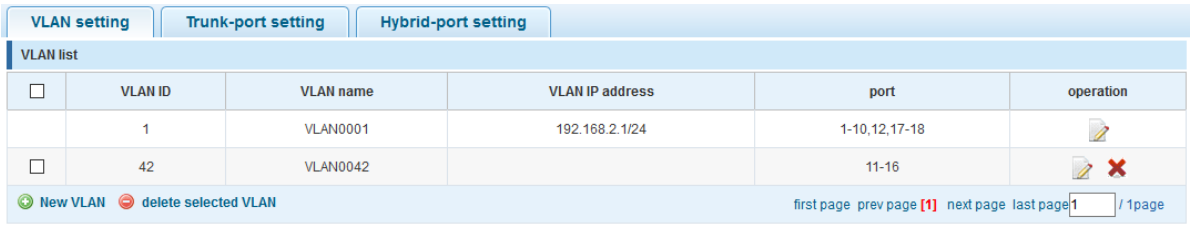


New VLAN:



Item	Description
VLAN ID	Type in the ID for the new VLAN. This value cannot be “1” nor any ID already setup on the switch.
VLAN Name	Provide a descriptive name for the VLAN (e.g., “VOICE”).
Choose to join the VLAN port	Select all the ports you wish to be a part of this VLAN. Note that these ports will act as access ports. They will add the VLAN ID to any untagged packet and reject any incoming packets that have a VLAN tag.

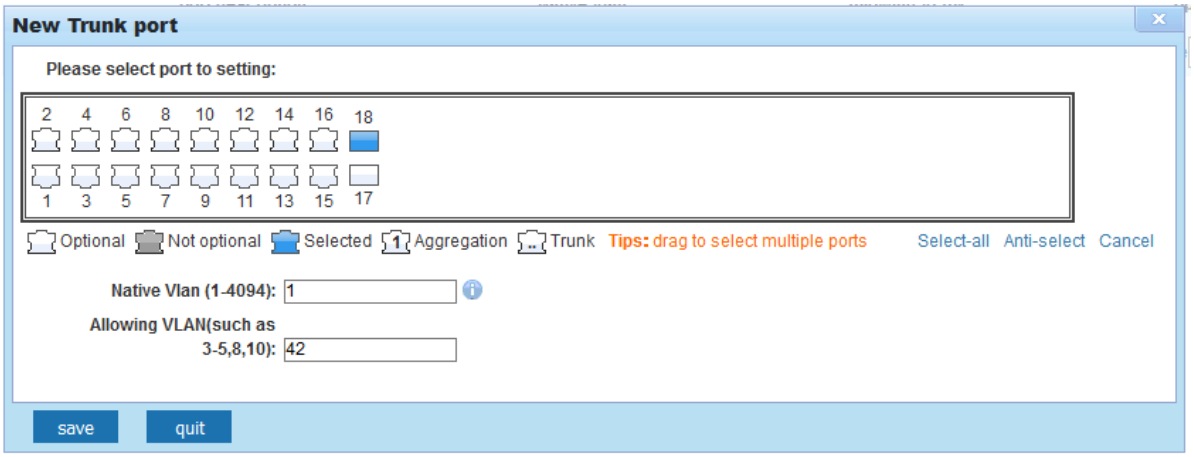
Note: VLAN ID 1 is the default VLAN, which cannot be removed. However, access ports that are assigned to another VLAN will be automatically removed from VLAN 1. The screen shot below shows what the setup looks like after the above VLAN has been added:



6.4.1 Trunk Port Settings

A trunk port transmits tagged packets and is used to connect different switches with one another.

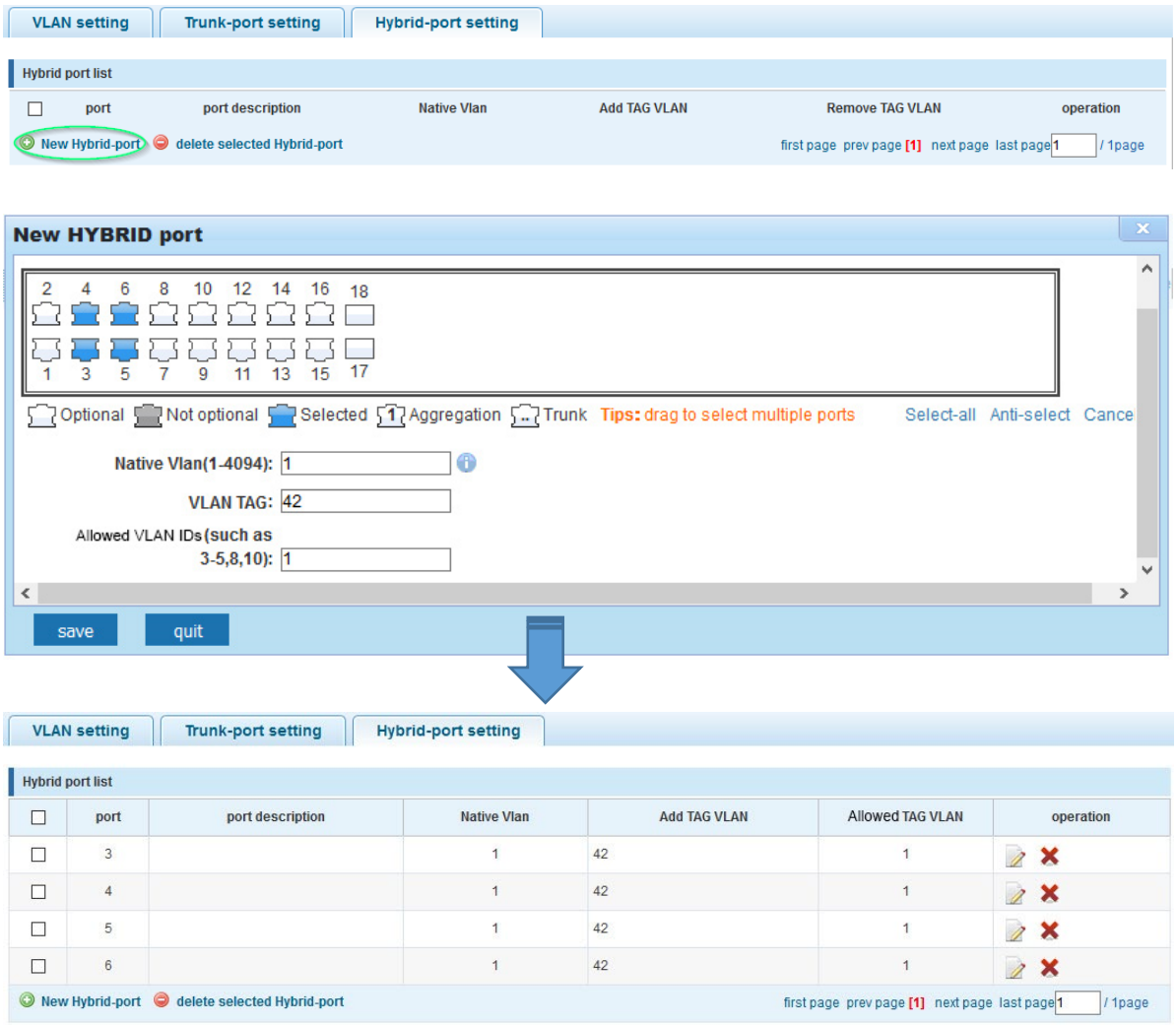
New Trunk-Port:



Item	Description
Native VLAN ID	The native VLAN ID is the untagged VLAN on an IEEE 802.1q trunked port. The native VLAN and management VLAN (see SYSTEM->SYSTEM CONFIG) can be the same, but in terms of security, it is better that they aren't. If a switch receives an untagged frame on a trunk port, it is assumed to be part of the Native VLAN that is designated on the switch trunk port.
Allowing VLAN	Enter the IDs of all VLANs, which you wish the trunk port to forward. All other tagged packets will be dropped. Note that any value you enter here must first be defined as a VLAN in the previous VLAN settings page.

6.4.2 *Hybrid Port Settings*

A Hybrid port is a combination of a trunk and an access port.

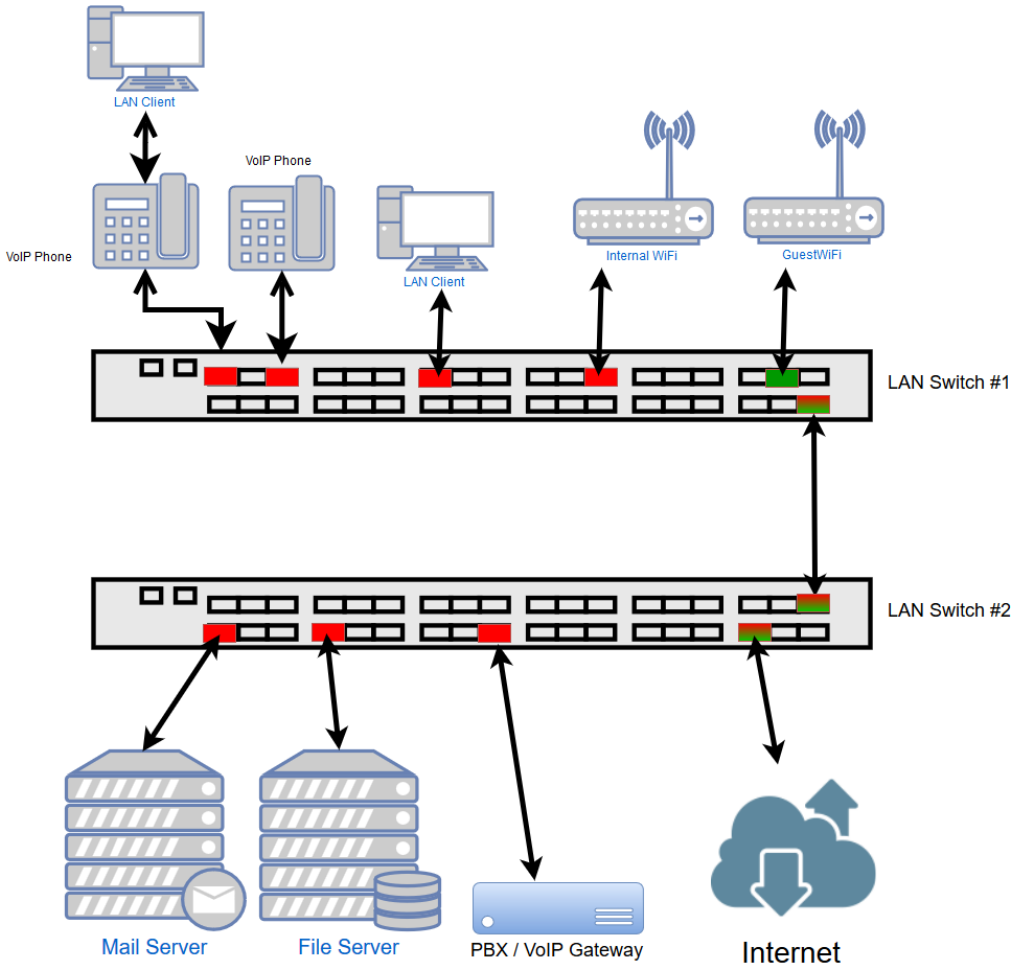


Item	Description
Native VLAN ID	See previous trunk port section.
VLAN TAG	VLAN ID that is added to any untagged packet arriving at the port. Note: You cannot enter multiple IDs or ranges of IDs. While the web interface may show this, it is incorrect.
Allowed VLAN IDS	Enter the IDs of all VLANs, which you wish the hybrid port to forward. All other tagged packets will be dropped.
Port Description	The name of the port as defined in section 6.3.1.
Add TAG VLAN	VLAN ID that is added to untagged VLAN packets.
Allowed TAG VLAN	Tagged VLAN packets that are allowed to pass through, all other tagged packets will be dropped.

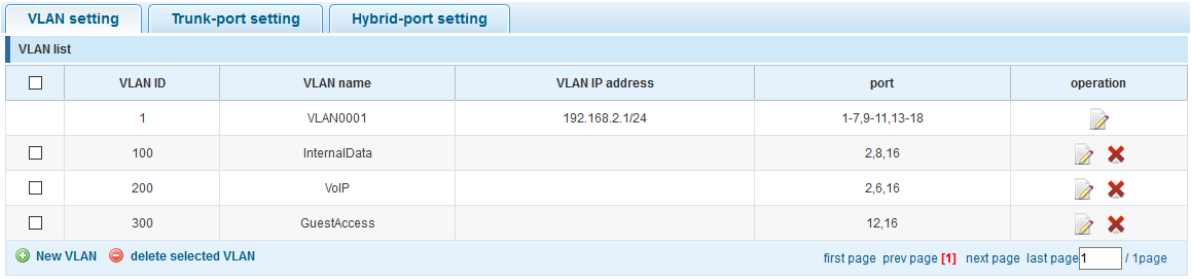
6.4.3 Setup Example

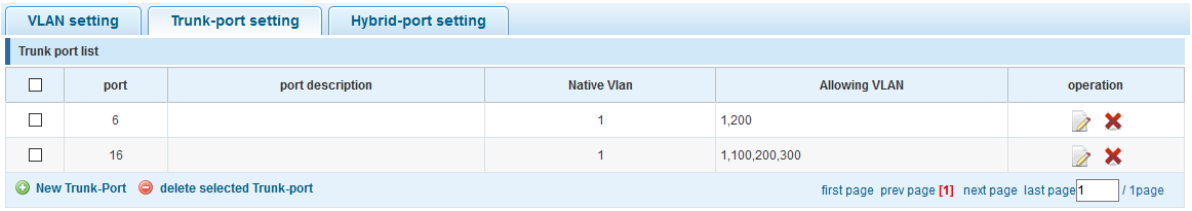
This section provides a real-life example and the corresponding setup of the Intellinet switch, or in this case, switches.

- There are three VLANs in the network
  - VLAN ID 100 – Internal data network with access to Internet
  - VLAN ID 200 –VoIP network
  - VLAN ID 300 – Guest network provides Internet access, but nothing else
- LAN Switch #1:
  - Port 2: VoIP phone using VLAN ID 200, PC connected to back of phone
  - Port 6: VoIP phone using VLAN ID 200
  - Port 8: PC
  - Port 10: Wireless access point for internal network and access to Internet
  - Port 12: Guest wireless access point provides Internet access only
  - Port 16: Connection to LAN switch #2
- LAN Switch #2:
  - Port 1: Connection to LAN switch #1
  - Port 2: Mail Server
  - Port 3: File Server
  - Port 4: VoIP Gateway / PBX
  - Port 8: Internet gateway, firewall, modem



6.4.3.1 *Set up LAN Switch #1:*

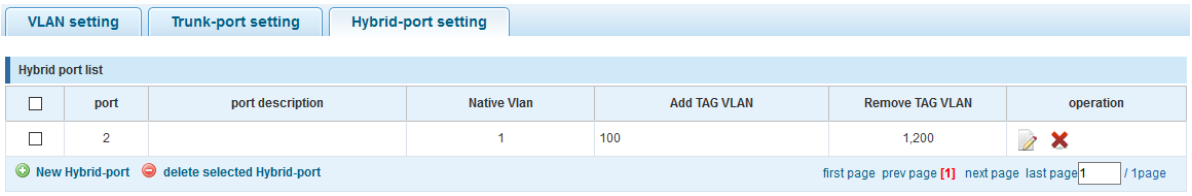




Trunk port settings:

Port 6: VoIP phone. This phone tags all packets by itself. The switch does not need to tag the packets.

Port 16: Connection to LAN switch #2. This port passes on all traffic for VLAN IDs 100, 200 and 300. All other traffic will be dropped.

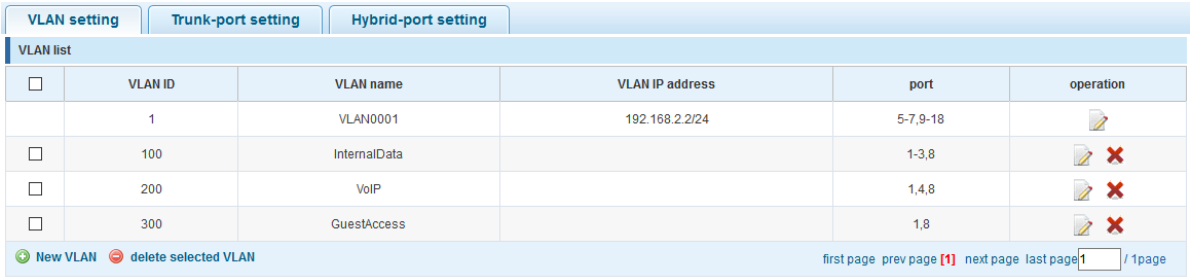


Hybrid port settings:

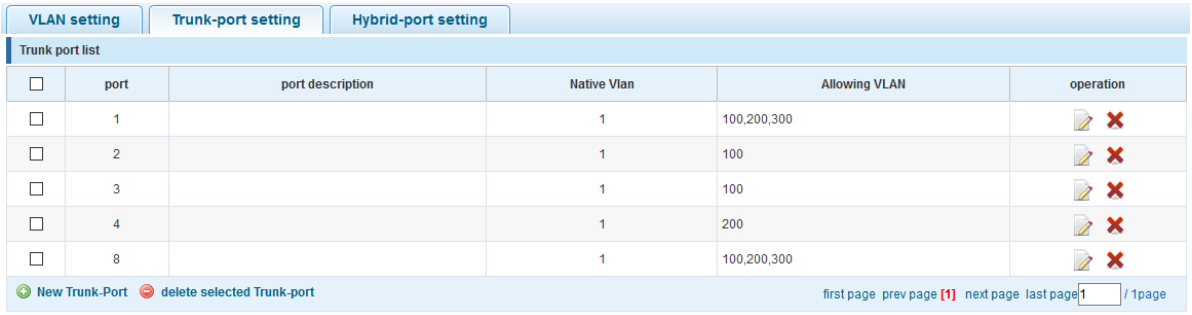
Port 2 is a special case because two networking devices are connected--the VoIP phone and a PC, which is connected to the back of the phone. The VoIP phone tags the packets itself, and the switch must let them go through, just like a normal trunk port would. However, the PC connected to it cannot tag the packets by itself and therefore must rely on the Intellinet switch to do so.

The Intellinet switch adds the VLAN ID 100 to all packets that are not tagged as VLAN ID 200. Port number two acts as an untagged port (VLAN ID 100) and tagged port (VLAN ID 200) at the same time, hence the name hybrid.

6.4.3.2 *Set up LAN Switch #2:*



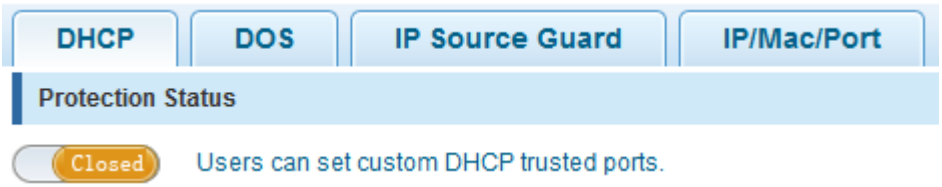
VLAN ID 1 (default VLAN) only contains ports that are not otherwise assigned.



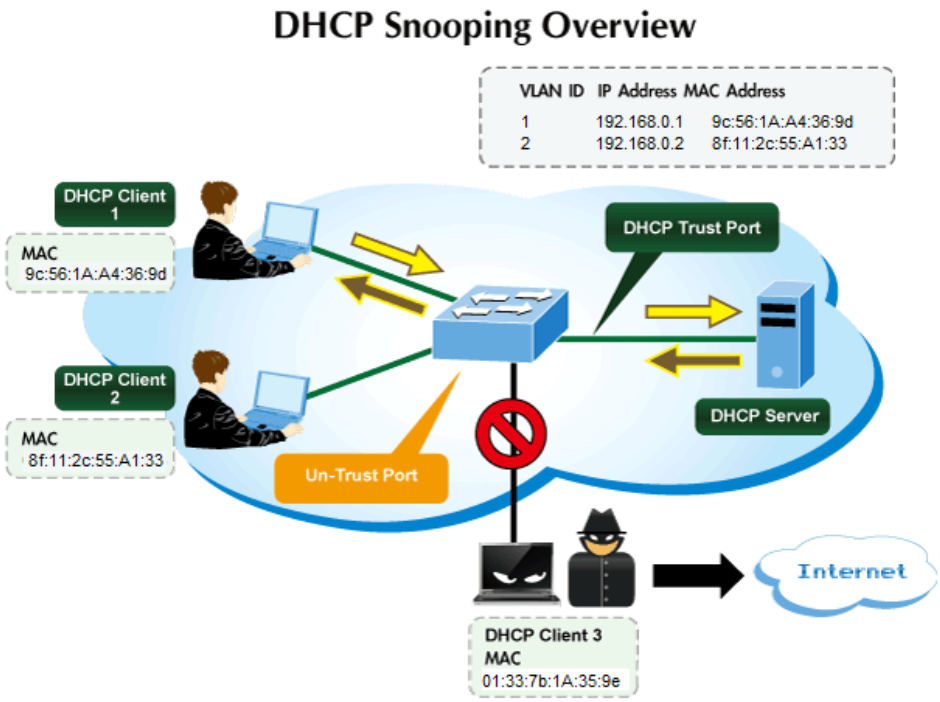
6.5 FAULT/SAFETY

6.5.1 Anti Attack

6.5.1.1 *DHCP Snooping*



DHCP snooping is a security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

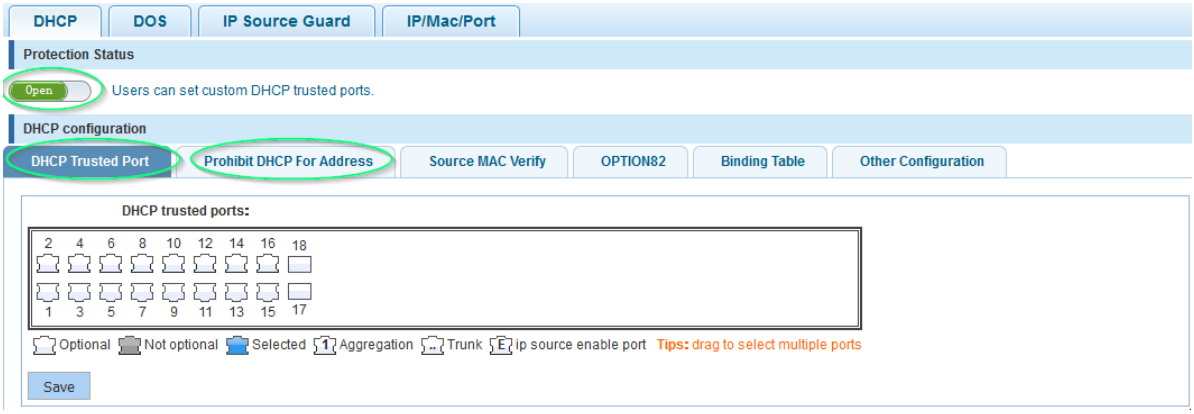


Command Usage

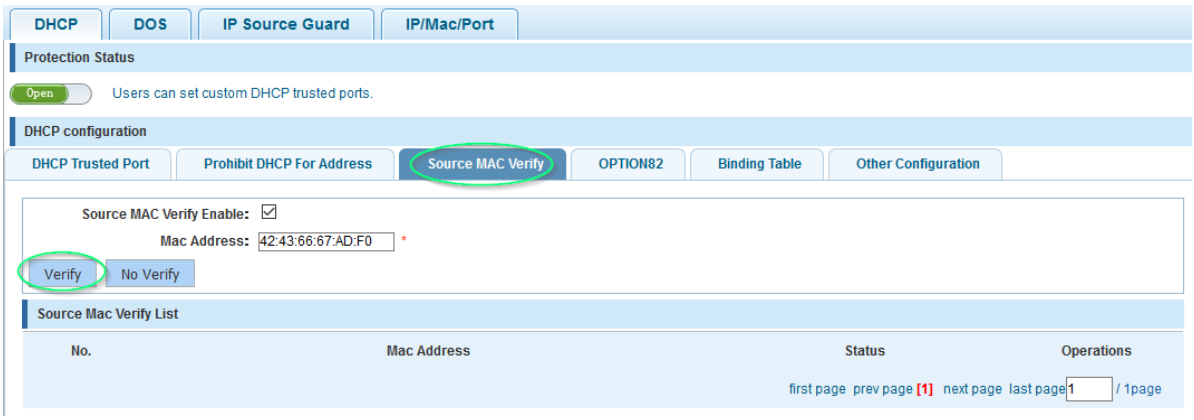
Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.

Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier and port identifier.

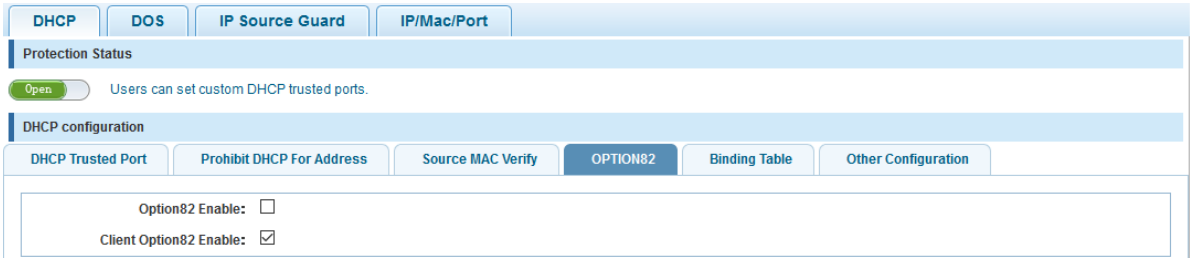
When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.



Item	Description
Native Protection Status	Closed: All DHCP related traffic will pass through the Intellinet switch without any interference. Open: Activates DHCP snooping. DHCP traffic is now subject to certain rules.
DHCP Trusted Port	These are trusted ports on your network, which are under your direct administrator control. Connected to these ports are typically switches, routers, and servers in the network. DHCP traffic from trusted ports is considered safe.
Prohibit DHCP For Address	Any port beyond the firewall or outside the network is untrusted. DHCP traffic from trusted ports is considered unsafe. DHCP response packets on these ports will be dropped, thus preventing a possible man-in-the-middle attack.

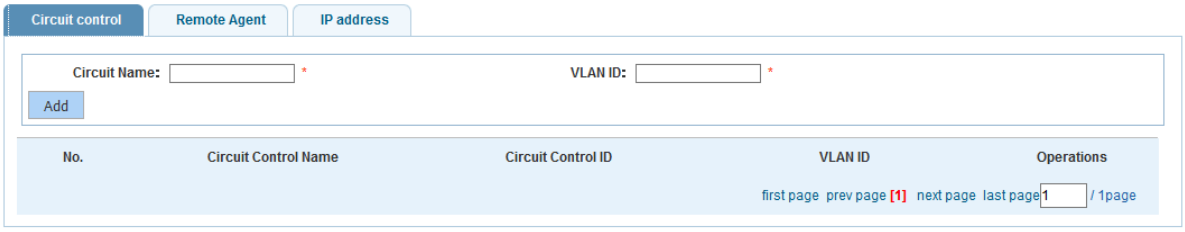


Item	Description
Source MAC Verify	DHCP snooping MAC address Verify ensures that the Intellinet switch verifies that the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports.
Source MAC Verify Enable	Check to activate MAC address verification.
MAC Address	Type in the MAC address (format xx:xx:xx:xx:xx:xx).
Verify / No Verify	Verify: Adds MAC address to the configuration. No Verify: Removes previously entered MAC address from configuration.



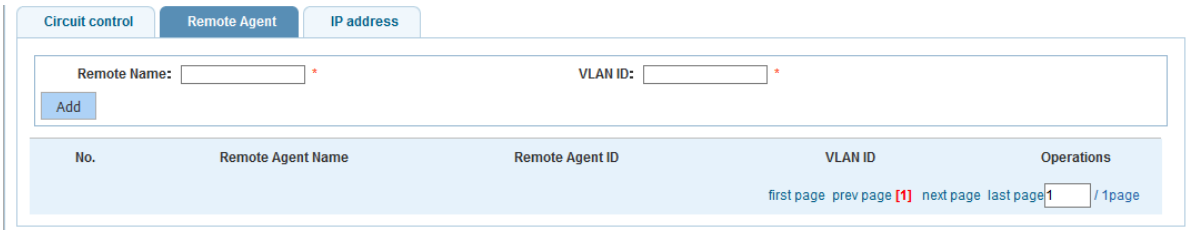
Enable Option82 support.

Client Option82 enabled trust mode.



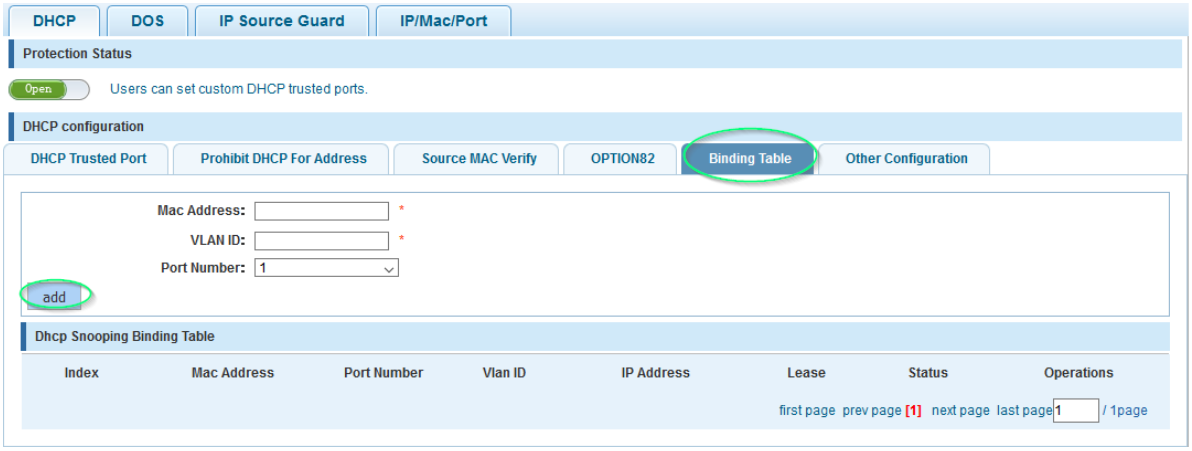
Option82 Agent Circuit ID (suboption 1)

Item	Description
Circuit Name	Circuit ID, an ASCII string that identifies the interface on which the client DHCP packet is received.
VLAN ID	Specify the Option82 for a specific VLAN ID (use 1 for default VLAN).



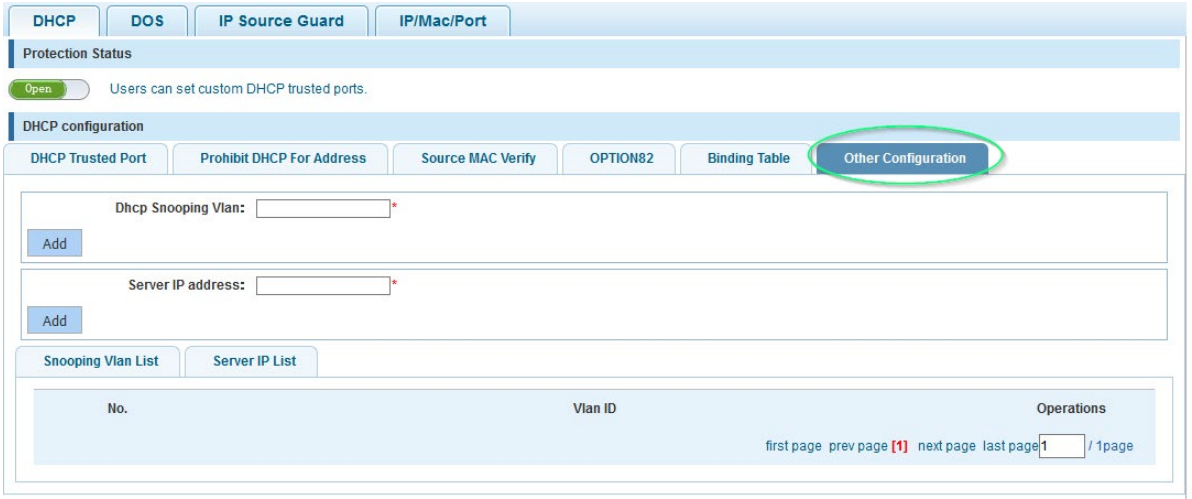
Option82 Agent Remote ID (suboption 2)

Item	Description
Remote Name	Remote ID, an ASCII string assigned by the DHCP relay agent that securely identifies the client.
VLAN ID	Specify the Option82 for a specific VLAN ID (use 1 for default VLAN).



When DHCP snooping is enabled, the lease information from the switching device is used to create the DHCP snooping database, also known as the DHCP snooping binding table. The table shows the IP-MAC binding, as well as the lease time for the IP address, type of binding, VLAN name and interface for each host. The information in this table is gathered during run-time as clients join the network and request IP addresses via DHCP. When the switch reboots, the information is lost, except for static bindings.

Item	Description
MAC Address	MAC address for static entry.
VLAN ID	Specify the VLAN ID for the static entry.
Port Number	Select the port (1 – 52) for the static entry.
DHCP Snooping Binding Table	Contains run-time information of connected DHCP clients, including their MAC address, the port number to which they are connected, the IP address they have been given, etc.



Item	Description
DHCP Snooping VLAN	VLAN to which you want to apply DHCP snooping.
Server IP Address	DHCP server IP address.

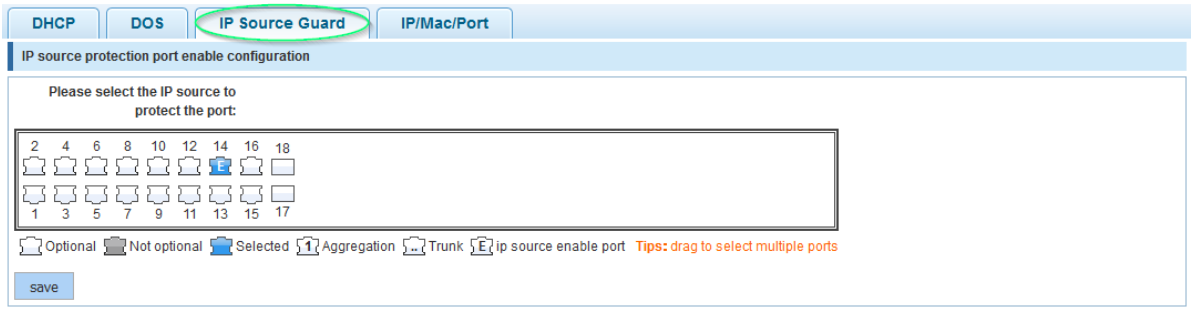
6.5.1.2 *DoS*

A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. The Intellinet switch has integrated mechanisms to counter possible DoS attacks, such as land attacks or illegal TCP/IP packets. There are configuration options. You simply activate or deactivate this feature.

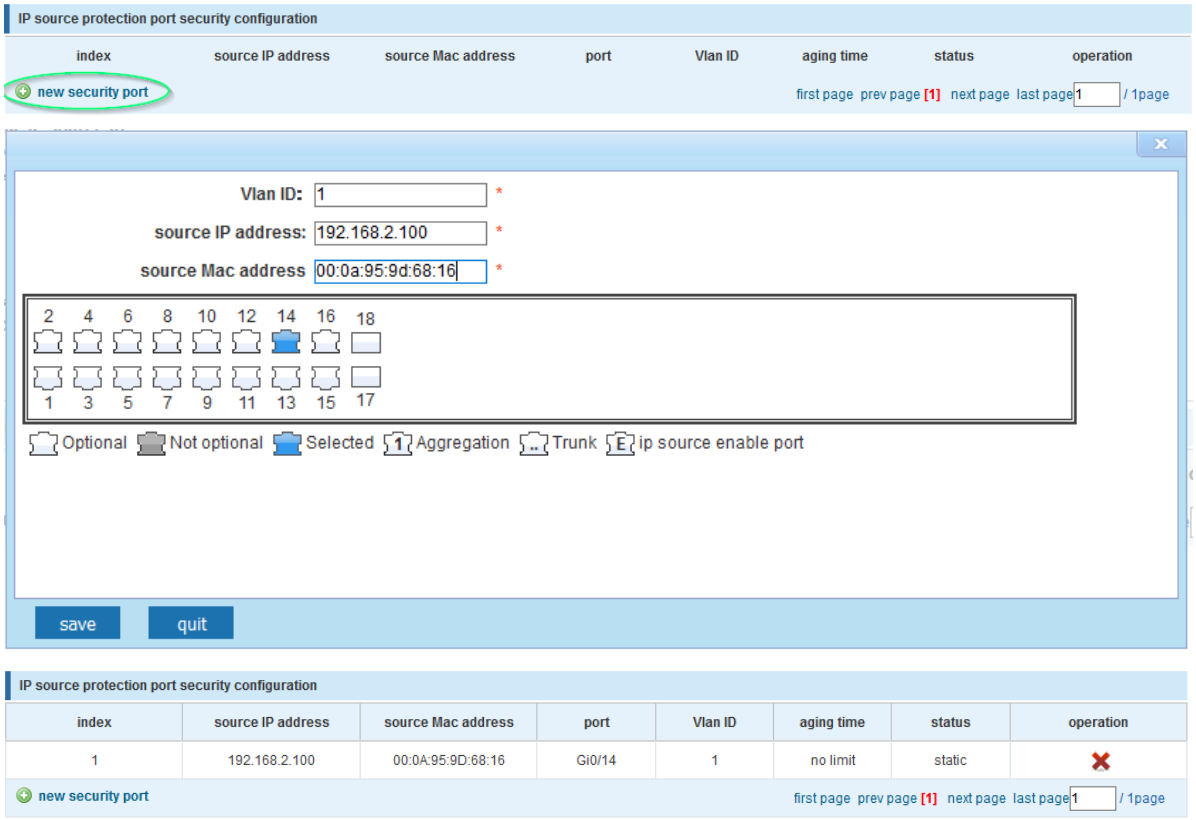
6.5.1.3 *IP Source Guard*

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding table (see section 6.5.1.1) or manually configured IP source bindings. Equipped with this feature, the Intellinet switch helps prevent IP spoofing attacks. An IP spoofing attack is when a host tries to spoof (fake) and use the IP address of another host in order to intercept traffic bound for that host.

If you enable IP Source Guard for a port initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server all traffic with that IP source address is permitted from that client. Instead of a DHCP server, it's possible to provide static IP source binding, which is called “new security port” on the Intellinet switch web admin UI.



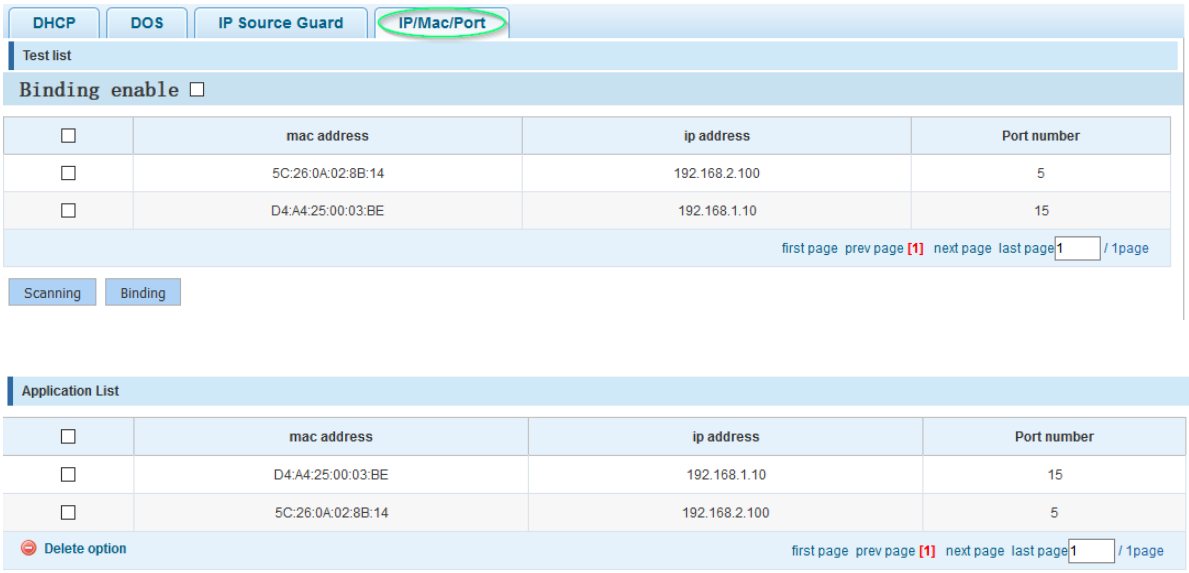
Item	Description
Please select the IP source to protect the port:	Select the port (or ports) that you wish to protect by IP Source Guard. The example above shows that IP Source Guard is enabled for port 14. Note that IP Source Guard isn’t supported on Trunk or aggregated ports.



Item	Description
VLAN ID	Specify the VLAN ID for the static entry. Leave 1 for the default VLAN.
Source IP Address	Specify the IP address of the client for the static entry.
Source MAC Address	Specify the MAC address of the client for the static entry.
Ports	Select the port to which the client is connected (port 14 in the example above). You can only select one port.

6.5.1.4 *IP MAC Port Binding*

The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch features IP-MAC-Port Binding. This is a powerful authentication function that ensures the correctness of hardware (MAC address), software/user (IP address), and location (Connected port) for devices connected to the network. This feature ensures they are all from legal sources to prevent the data leakage from hackers faking the legal network devices.

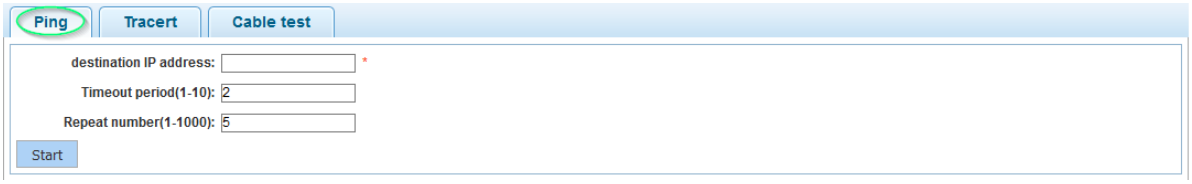


Item	Description
Binding Enable	Check to activate IP Mac port binding.
Scanning	Click to scan for connected network clients.
Binding	Select the clients you wish to add to the IP Mac port binding table, then click on “Binding”.
Application List	All current, static IP-MAC-port binding entries are listed here. Note that this information will be lost after the switch is restarted.

6.5.2 Channel Detection

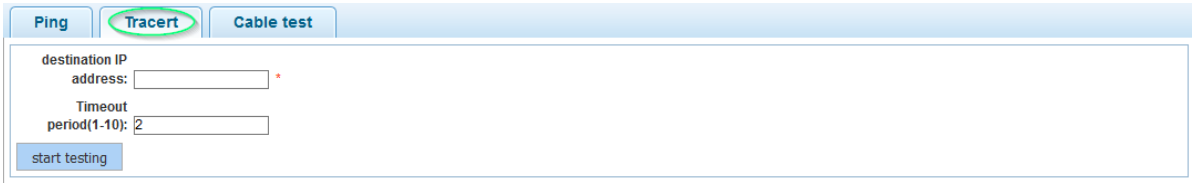
The Intellinet switch is equipped with a set of network tools that can aid the network administrator in troubleshooting problems.

6.5.2.1 *Ping*



Item	Description
Destination IP address	IP address you wish to ping.
Timeout Period	Define the maximum allowed response time(s) before the response is considered to have timed-out.
Repeat number	Define how many ping requests you want the Intellinet switch to send to the destination IP address.

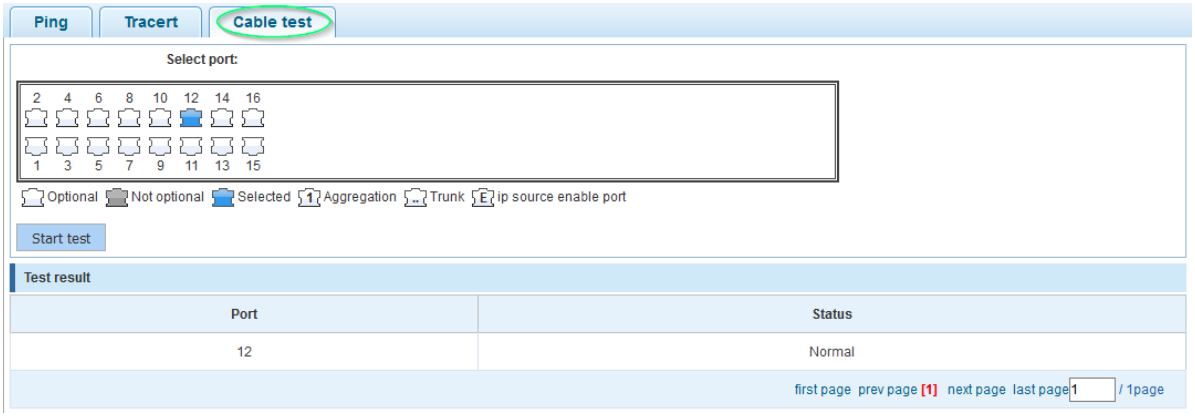
6.5.2.2 *Tracert*



Item	Description
Destination IP address	IP address you wish to run a tracert for.
Timeout Period	Define the maximum allowed response time(s) before the response is considered to have timed-out.

6.5.2.3 *Cable Test*

The cable test utility allows a quick check of the connected cables.



Item	Description
Select Port	Select one of the 18 ports, then click on “Start test.”
Test Results	Displays the results of the cable test. Note that if you test a port to which no cable is connected, the test returns the value “circuit breaker.”

6.5.3 *ACL Access Control List*

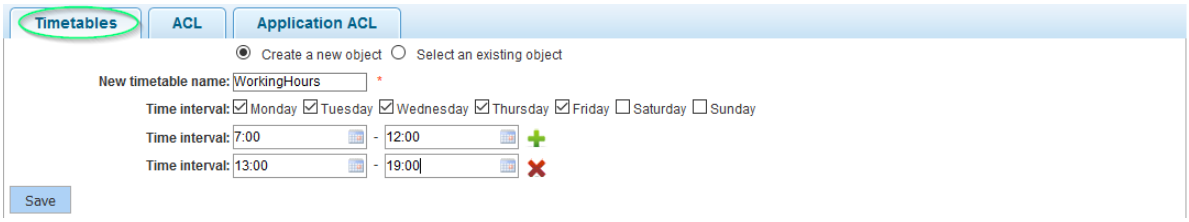
ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

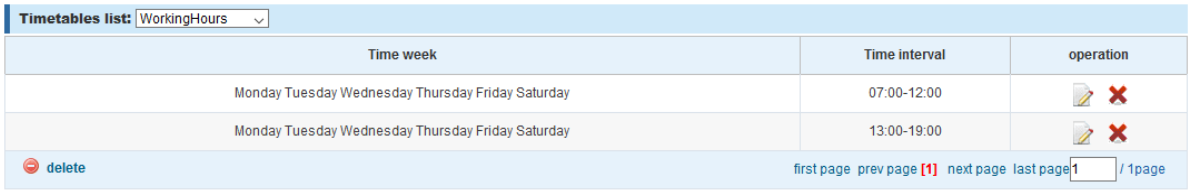
ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex; for example, when the ACEs are prioritized for various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

6.5.3.1 *Timetables*

This section allows you to set up a time frame. This time frame can be applied to ACL rules to either allow or deny access. The time table does not directly specify whether access is denied or allowed. Rather, it is simply a way to create an easily accessible time frame that can be applied to ACL rules. The example below shows the setup of a timetable called “WorkingHours.” Note that the Intellinet switch must be set up with a proper system time (see section System Config).

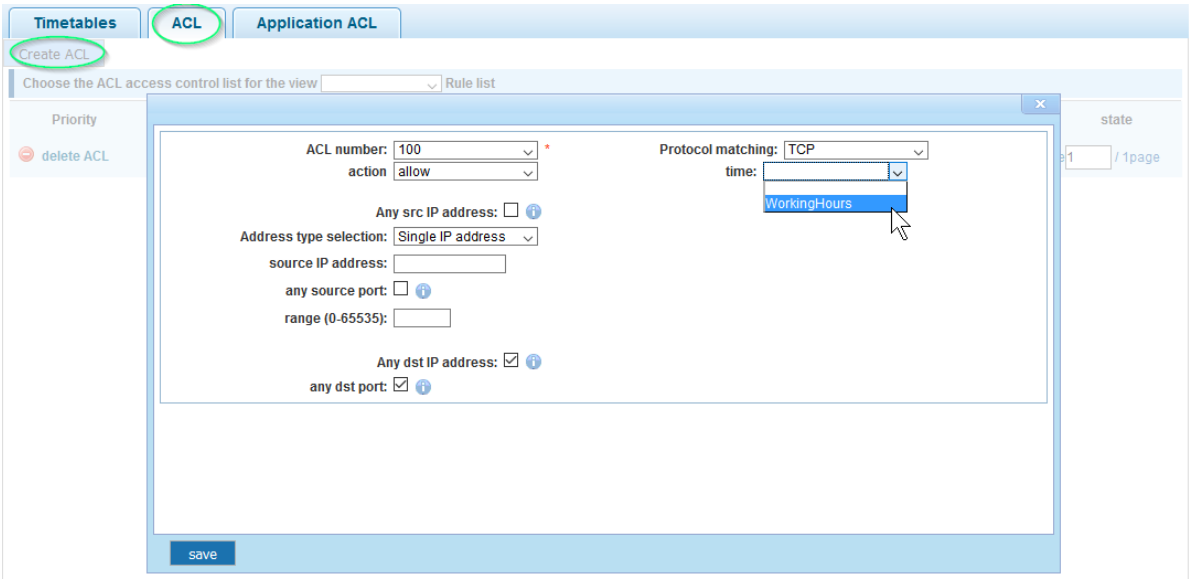




Item	Description
New Timetable Name	Provide a descriptive name for the timetable.
Time Interval	Specify the days of the week and start and end time. Click on the to add additional time frames. Click “Save” to save the timetable.
Timetables list	Drop-down list contains all timetables previously set up.
Time week	Selected weekdays for the selected timetable.
Time Interval	Time interval for selected timetable.
Operation	Edit selected timetable Deled selected timetable

6.5.3.2 *ACL*

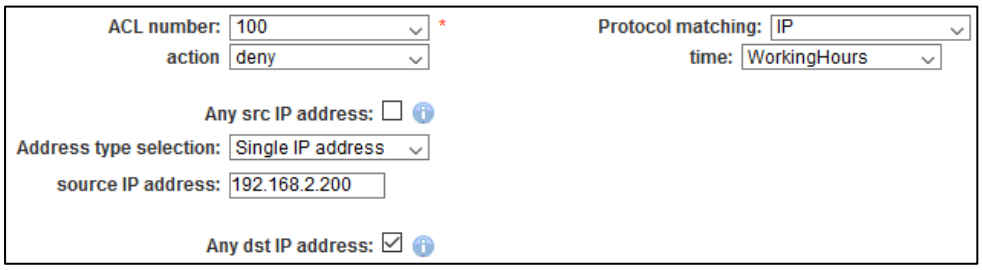
In this section, set up the actual access control list (ACL). The ACL connects IP address and port information with a timetable (see section 6.5.3.1) and an action to either allow or deny access to the network through the switch. The example below creates an ACL, which allows access to the network for any computer



Item	Description
ACL Number	Each ACL rule gets a number. Select the one from the drop-down list for which you want to create this ACE (Access Control Entry).
Action	Define whether this rule grants access (“allow”) to the network, or prohibits it (“deny”).
SRC/DEST IP Address	Specify the source and destination IP address for this ACE. You can provide a single IP address (e.g., 192.168.2.100) or a specific network (e.g., 255.255.255.0).
SRC/DEST Port	This option is only visible if the ACE is created for TCP or UDP. It will not show for IP ACLs (see next parameter). You can provide a single port or a range of ports.
Protocol Matching	IP: The ACE is applied to packets based on their source and/or destination IP address. TCP/UDP: The ACE is applied to packets based on their source and/or destination IP address and the port number for the selected protocol.
Time	If you want to limit the ACE to a specific timetable (see section 6.5.3.1), you can select it from the drop-down list.

Example 1 – Disallow access to the network for any computer outside of the working hours.

Example 2 – Disallow access to the network for an individual IP address during the working hours.



6.5.3.3 *Application ACL*

With this function you can link an ACL to one or more of the 18 available switch ports.

Select the ports and ACL list, and click “Save” in order to activate.

6.6 Spanning Tree Protocol (STP)

The Spanning Tree Protocol can be used to detect and disable network loops and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network. It also provides backup links, which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention. This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation to network performance if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch. When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

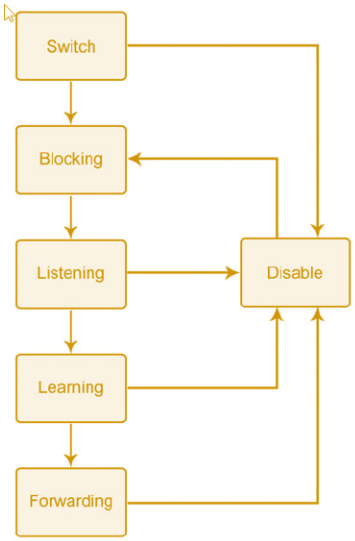
BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- Blocking – the port is blocked from forwarding or receiving packets
- Listening – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- Learning – the port is adding addresses to its forwarding database, but not yet forwarding packets
- Forwarding – the port is forwarding packets
- Disabled – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

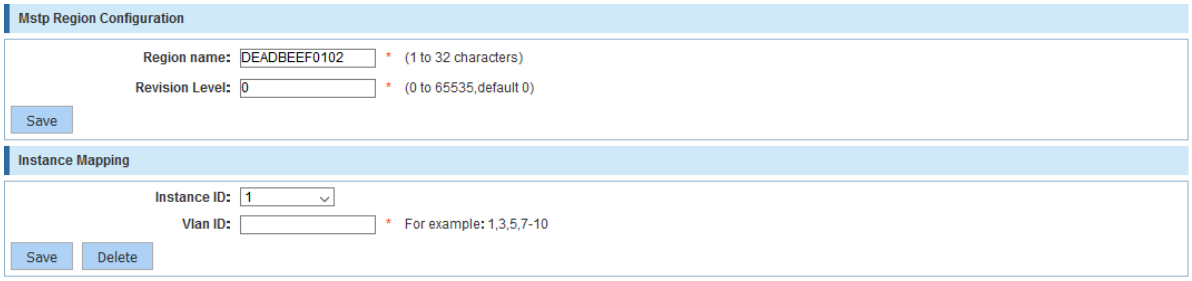
- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking



It's possible to modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from or received by STP enabled ports, until the forwarding state is enabled for that port.

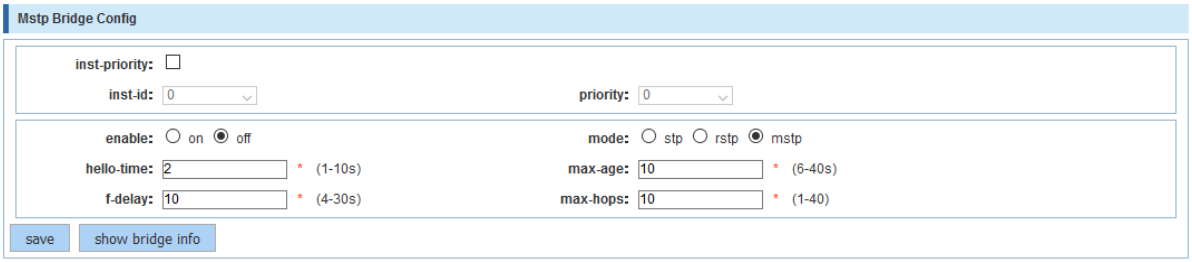
The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

6.6.1 MSTP Region

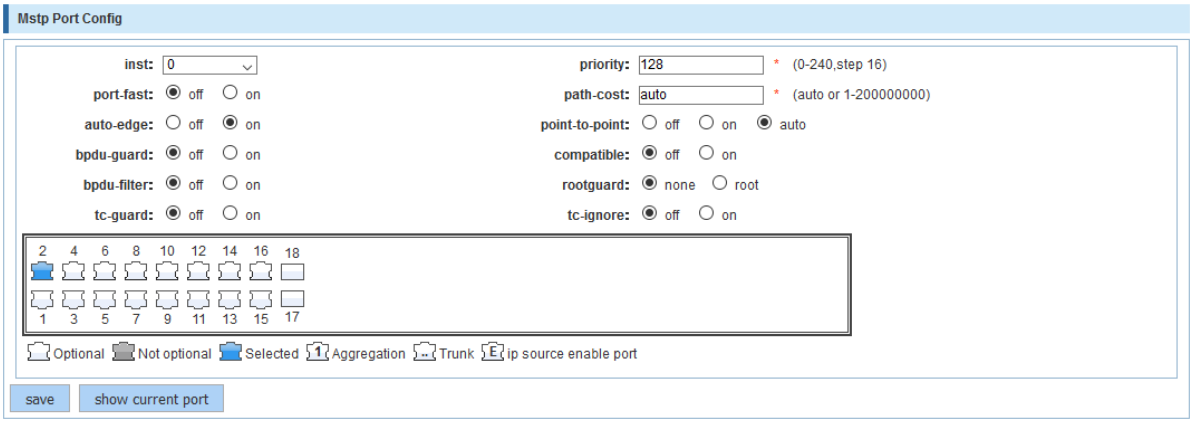


Item	Description
MSTP Region Configuration	Each switch running MST in the network has a single MST configuration that consists of these two attributes: 1. Region name a. An alphanumeric configuration name 2. Revision Level
Instance Mapping	A table that associates each of the potential 4096 VLAN IDs to a given instance.

6.6.2 *MSTP Bridge*



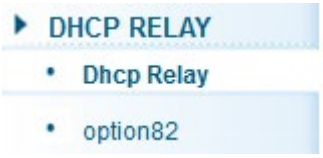
Item	Description
inst-priority	Priority can be configured for a specified instance.
inst-id	Select the instance ID for which you want to define a priority.
Priority	Select the priority level for the instance ID.
Enable	Enable / disable STP.
Mode	• STP – Spanning Tree Protocol (IEEE 802.1D) • RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w) • MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)
Hello-time	The hello timer is the time interval between each Bridge Protocol Data Unit (BPDU) that is sent on a port. The default hello timer is 2 seconds. Adjust the Spanning Tree Protocol (STP) hello timer to any value between 1 and 10 seconds.
f-delay	The forward delay timer is the time interval that is spent in the listening and learning state. The default forward delay timer is 10 seconds. Set the Spanning Tree Protocol (STP) forward delay timer to any value between 4 and 30 seconds.
Max-age	The max age timer controls the maximum length of time interval that an STP switch port saves its configuration Bridge Protocol Data Unit (BPDU) information. The default max age timer is 10 seconds. Adjust the max age timer to any value between 6 and 40 seconds.
Max-hops	For Multiple Spanning Tree Protocol (MSTP), configure the maximum number of hops a BPDU can be forwarded in the MSTP region. The default value is 10. Possible values range from 1 to 40.



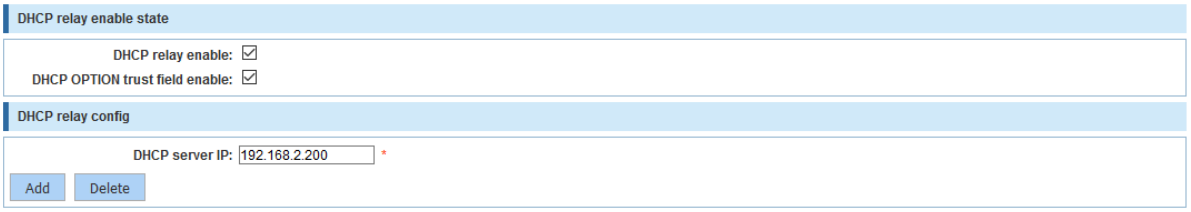
Item	Description
inst	Select the instance ID.
port-fast	The time Spanning Tree Protocol (STP) takes to transition ports over to the forwarding state can cause problems. Port-fast is a function to resolve this problem. Port-fast solves the problem of delays when client computers are connecting to switches. With port-fast enabled on a port, you effectively prevent the implementation of STP on that port.
auto-edge	By default, “auto-edge” is enabled on all ports. This will look for BPDUs for 3 seconds and, if none are found, will begin forwarding packets, and the port is set as “edge.” If there are BPDUs, the port is set as “non-edge.”
bdpu-guard	BPDU guard disables the port upon BPDU reception if port-fast is enabled on the port. This effectively denies devices connected to these ports from participating in the designed STP, thus protecting your data-center core.
bdpu-filter	Enabling BPDU filtering for a port stops sending or receiving BPDU on this interface; this is the same as disabling spanning tree on the interface. It is a risky choice, unless you are sure that no switch can ever be connected to this port.
tc-guard	In certain situations it can be desirable to prevent topology changes originating at or received at a given port from being propagated to the rest of the network. This may be the case when the network is not under a single administrative control and it is beneficial to prevent devices external to the core of the network from causing MAC-address flushing in the core. This behavior can be enabled by configuring Topology Change Guard (TC Guard) on the port.
priority	If a loop occurs in the network, MSTP uses the port priority parameter when selecting an interface to put into the forwarding state. Assign higher priority values (lower numbers) to interfaces that you want selected first and lower priority values (higher numbers) that you want selected last. If all interfaces have the same priority value, MSTP puts the port with the lowest interface number in the forwarding state and blocks the other ports.
path-cost	The MSTP path cost default value is derived from the media speed of an interface. If a loop occurs, MSTP uses cost when selecting an interface to put in the forwarding state. Assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
point-to-point	Admin Point-to-Point Link--Specify whether this port is connected to a shared LAN segment (value “off”) or a point-to-point LAN segment (value “on”). A point-to-point LAN segment is connected to exactly one other bridge (normally with a direct cable between them). Only point-to-point links and edge ports can rapidly transition to forwarding state. If you set this value to “auto,” the switch automatically detects whether the port is connected to a shared link or a point-to-point link.
Rootguard	Root-guard ensures that an unintended switch does not become a new root bridge. Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.
tc-ignore	Ignore technology change (TC) on or off.

6.7 DHCP Relay Agent

A DHCP client is an Internet host using DHCP to obtain configuration parameters such as an IP address. A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. The Intellinet switch can fulfill the role of such a relay agent.



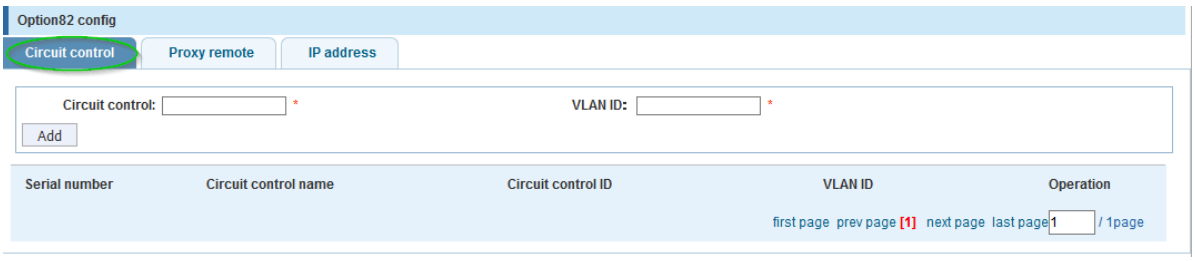
6.7.1 DHCP Relay



Item	Description
DHCP relay enable	Enable or disable DHCP relay.
DHCP OPTION trust field enable:	When enabled, the client that receives the DHCP message with option82 information will forward it; otherwise, it will be discarded.
DHCP Server IP	Provide the IP address of the DHCP server, and click “add.”

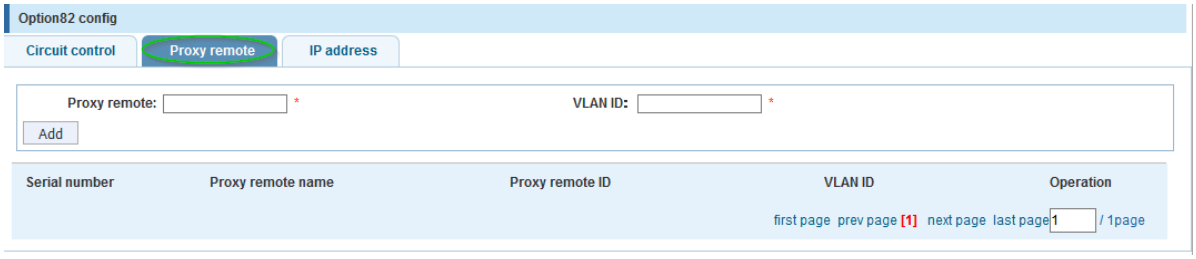
6.7.2 Option82

6.7.2.1 *Circuit Control*



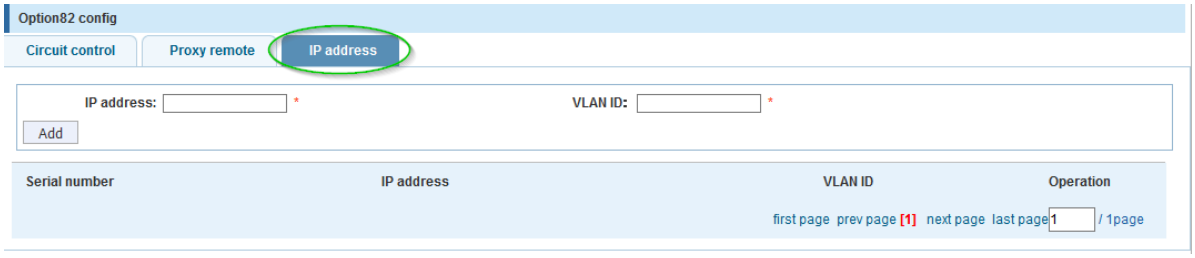
Item	Description
Circuit Control	Provide the circuit ID number. Possible values range from 3 to 63.
VLAN ID	Type in the VLAN ID. Use value 1 for the default VLAN..

6.7.2.2 *Proxy Remote*



Item	Description
Proxy Remote	ASCII Remote ID string, up to 63 characters.
VLAN ID	Type in the VLAN ID. Use value 1 for the default VLAN.

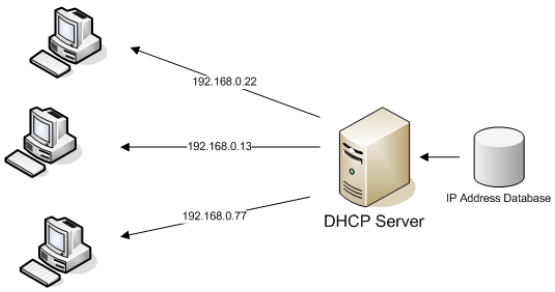
6.7.2.3 *IP Address*



Item	Description
IP Address	IP address of DHCP server.
VLAN ID	Type in the VLAN ID. Use value 1 for the default VLAN.

6.8 DHCP SERVER

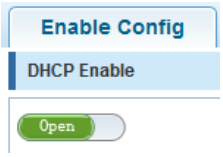
The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters such as IP addresses for interfaces and services. A typical DHCP server is a router or a Windows server. The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch can also fulfill the role of a DHCP server.



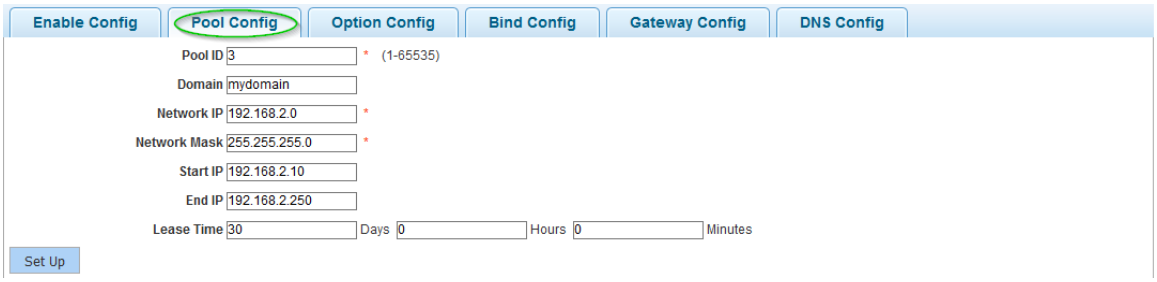
6.8.1 DHCP Config

6.8.1.1 *Enable Config*

Set this option to “Open” in order to activate the DHCP server function. Note that when you want to use the DHCP Server function, you cannot use the DHCP relay feature (see section6.7 DHCP Relay Agent) at the same time.



6.8.1.2 *Pool Config*

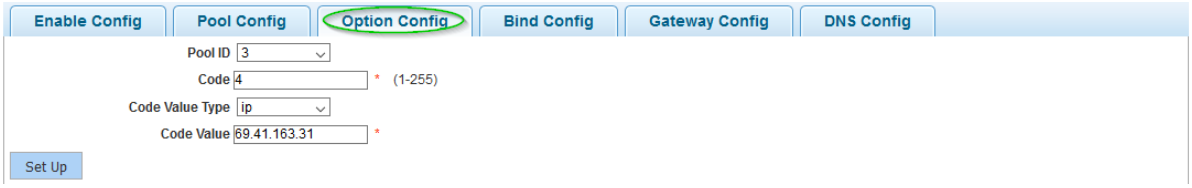


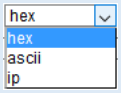
Item	Description
Pool ID	Identifies the dynamic address pool from which the DHCP requests are served.
Domain	If you are on a domain network, the domain name should go here.
Network IP	This is the first IP address of the subnet ending in “.0”. It can’t be assigned to an actual network client.
Network Mask	Provide the network mask of choice for your network.
Start IP	Define the lowest IP address of the IP address pool.
End IP	Define the highest IP address of the IP address pool.
Lease Time	Defines how long the client is allowed to keep the IP address. When the time has elapsed, the switch will issue a new IP address to the client.

Note: The DHCP IP address range must be in the same range as the Intellinet switch's LAN IP range (e.g., 192.168.2.xxx).

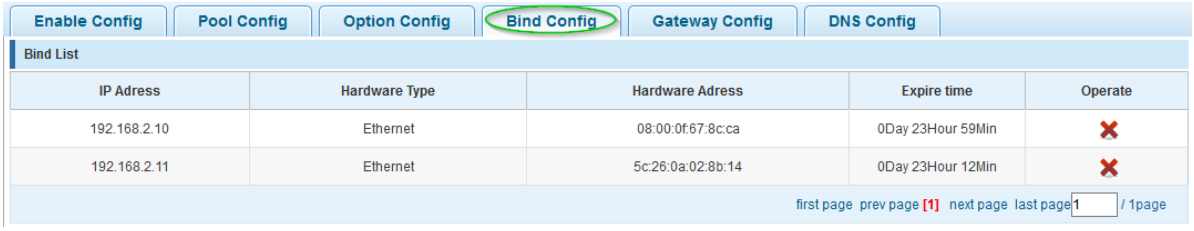
6.8.1.3 *Option Config*

This page allows modification of the DHCP options, as stated in RFC2132. The example below shows how to specify a specific NTP server.



Item	Description
Pool ID	Identifies the dynamic address pool from which the DHCP requests are served.
Code	Possible values are – to 255. These are the codes or tags per RFC2132.
Code Value Type	 Select the appropriate value (i.e., select IP if you enter an IP address in the code value field below).
Code Value	Provide the value fort the tag (code) you selected.

6.8.1.4 *Bind Config*



This page displays all clients that have obtained an IP address from the Intellinet switch. Click on to set the lease time to expired, forcing the connect client to obtain a new IP address instantly.

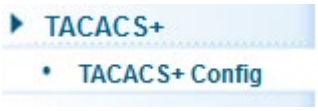
6.8.1.5 *Gateway Config*

On this page, provide the Gateway IP address that you wish to provide to the DHCP clients.

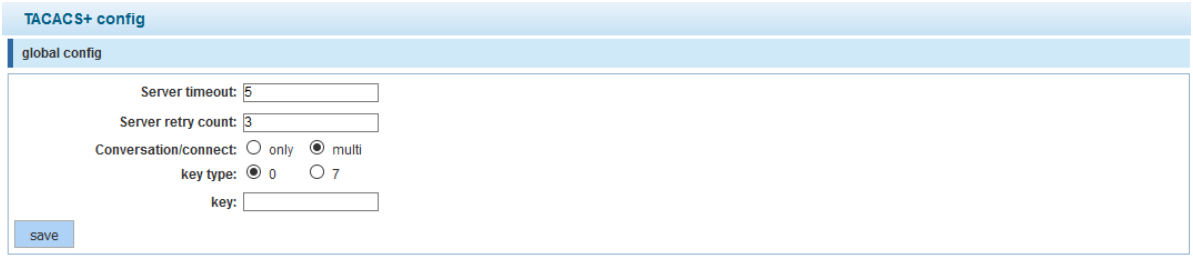
6.8.1.6 *DNS Config*

On this page, provide the DNS IP address(es) that you wish to provide to the DHCP clients.

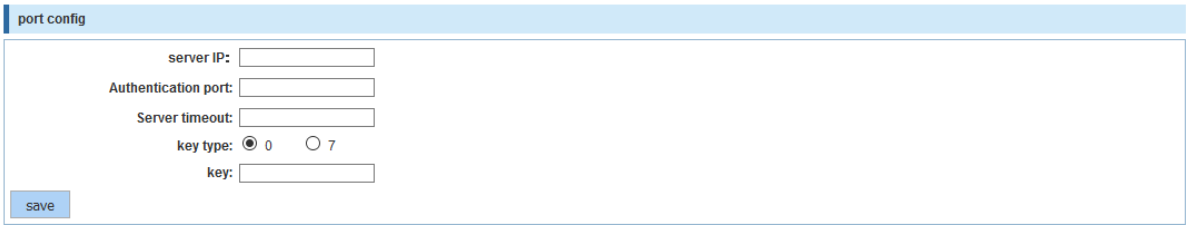
6.9 Terminal Access Controller Access-Control System (TACACS+)



Terminal Access Controller Access-Control System (TACACS, usually pronounced like "tack-axe") refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server. The original TACACS protocol, which dates back to 1984, was used for communicating with an authentication server, common in older UNIX networks; it spawned related protocols. Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol released as an open standard beginning in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles authentication, authorization and accounting (AAA) services. Compared to the open standard RADIUS authentication (section 6.10 Radius), TACACS+ encrypts the entire payload whereas RADIUS only encrypts passwords.

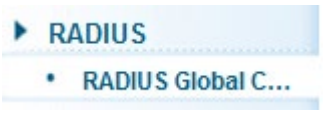


Item	Description
Global Config	Global parameters that can be overwritten by port-specific configuration.
Server timeout	The global timeout interval determines how long the Intellinet switch waits for responses from TACACS+ servers before declaring a timeout failure.
Server retry count	Specifies the number of retry attempts that will be made to establish a Transmission Control Protocol (TCP) connection between a TACACS+ client and the TACACS+ server. The default value is 3.
Conversation / Connect	This parameter defines how many connections there will be between router daemon. Only: “single-connection" The daemon must support single-connection mode for this to be effective; otherwise, the connection between the network access server and the daemon will lock up or you will receive spurious errors.
Key type	0: Key value in clear text format 7: Key value is type-7 encrypted.
Key	Type in the key value.



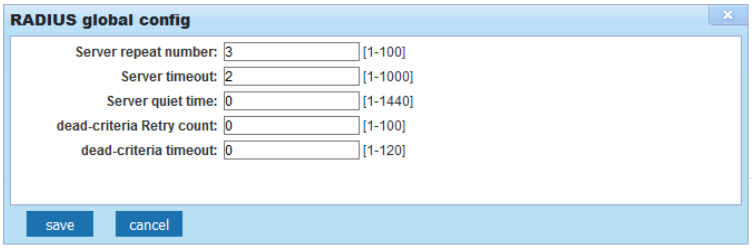
Item	Description
Port Config	Global parameters that can be overwritten by port-specific configuration.
Server IP	IP Address for the TACSACS+ server.
Authentication port	Define the TCP port number of the TACSACS+ server connection.
Server timeout	The timeout interval determines how long the Intellinet switch waits for responses from a specific TACACS+ server before declaring a timeout failure. If left empty, the global server timeout value will be used; otherwise, the server timeout takes precedence.
Key type	0: Key value in clear text format 7: Key value is type-7 encrypted.
Key	Key value.

6.10 RADIUS



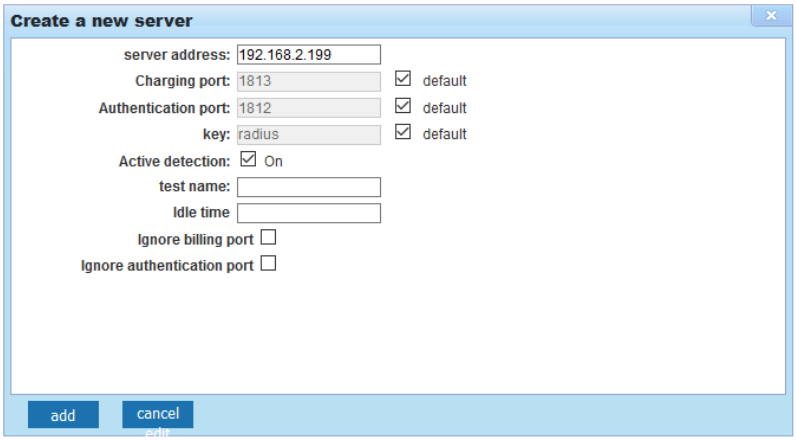
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS is a client/server protocol that runs in the application layer and can use either TCP or UDP as transport. Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication as well. The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server.

6.10.1 Radius General Config



Item	Description
Server repeat number	Specifies the number of retry attempts that will be made to establish a connection between a RADIUS client and the RADIUS server. The default value is 3.
Server timeout	The timeout interval determines how long the Intellinet switch waits for responses from RADIUS server before declaring a timeout failure.
Server quiet time	If the Intellinet switch is unable to authenticate the client, it'll wait a specified amount of time before trying again. The amount of time is specified with the quiet-period parameter. Entered in minutes; max. 1440 minutes (24 hours).
Dead-criteria retry count	Set the number of times that the Intellinet switch does not get a valid response from the RADIUS server before the server is considered unavailable.
Dead-criteria timeout	Set the time in seconds during which the Intellinet switch does not need to get a valid response from the RADIUS server. The range is from 1 to 120 seconds.

6.10.2 Radius Server Config



Item	Description
Server address	Type in the address of the RADIUS server.
Charging port	Type the accounting port number on the RADIUS server's host computer. The default port number is 1813.
Authentication port	Type the accounting port number on the RADIUS server's host computer. The default port number is 1812.
Key	The key parameter in the radius-server command is used to encrypt RADIUS packets before they are sent over the network. The value for the key parameter on the Intellinet switch device should match the one configured on the RADIUS server. The default value is "radius".
Active detection	Enables or disables active detection of RADIUS server.
Test name	The user name for active detection.
Idle time	The interval time for RADIUS security server send message on accessible state. The default value is 60 minutes. Possible values range from 0 to1440 minutes (24 hours).

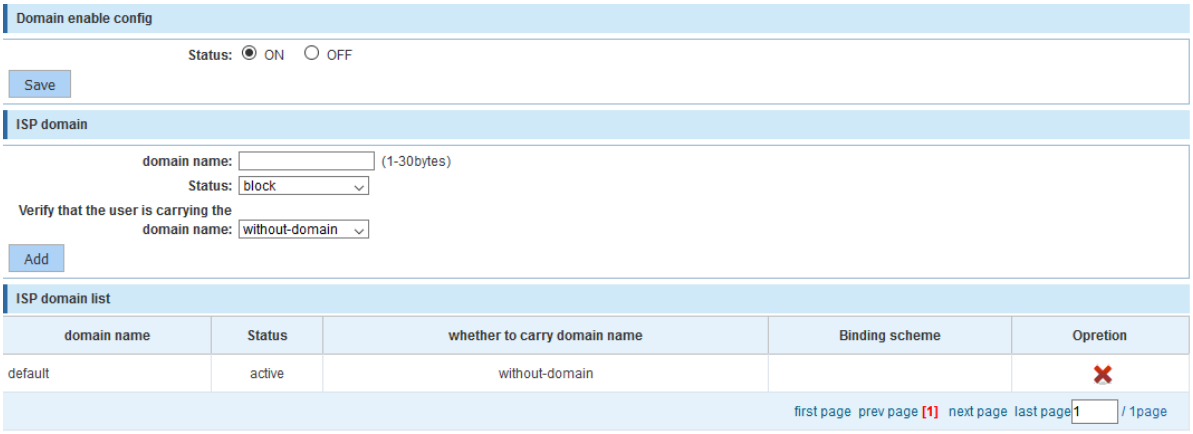
6.11 AAA

Authentication, authorization and accounting (AAA) is a system for tracking user activities on an IP-based network and controlling their access to network resources. AAA is often is implemented as a dedicated server.

6.11.1 Enable Config

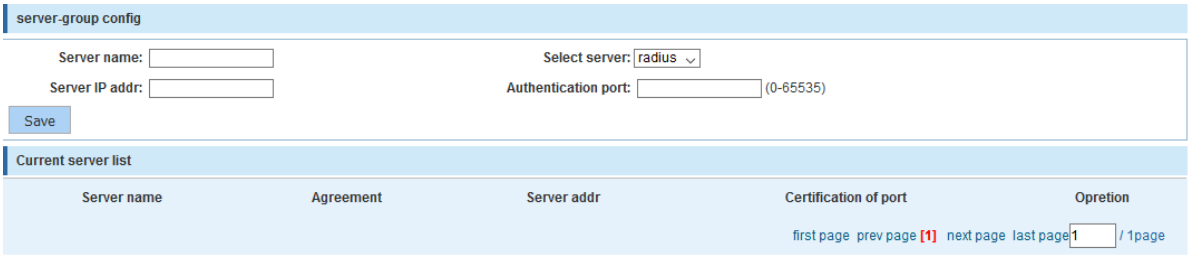
Enable or disable AAA.

6.11.2 Region Config



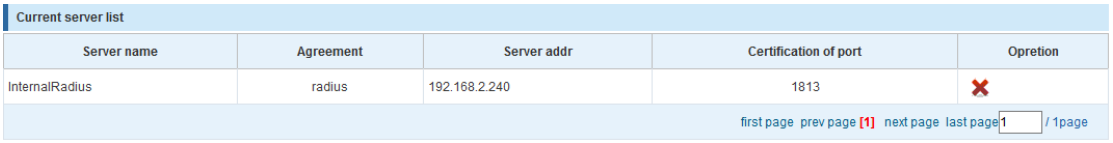
Item	Description
Domain name	Type in the name of the ISP domain. An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a user name in the format of userid@isp-name or userid.isp-name, the isp-name following the "@" or "." character is the ISP domain name. The access device uses userid as the user name for authentication, and isp-name as the domain name.
Status	Set to either "block" or "active." By default, an ISP domain is in the active state, which means that all the users in the domain are allowed to request network service.
Verify that the user …	Verify that the user is carrying the domain name.

6.11.3 Server Config



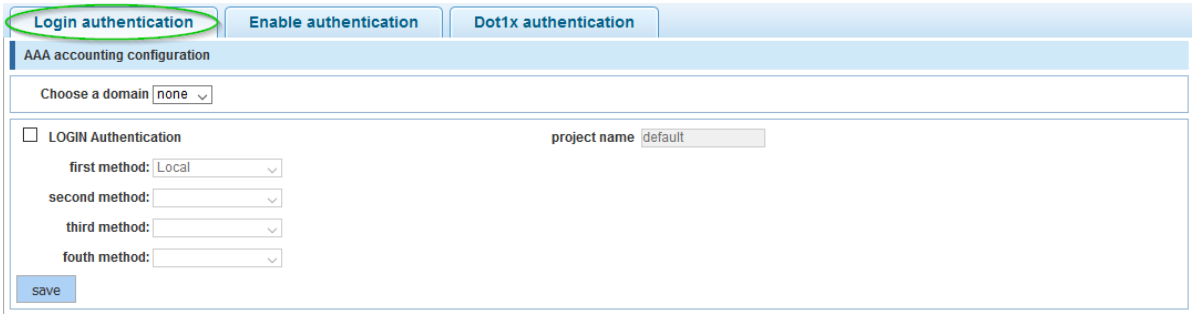
Item	Description
Server name	Type in the name for the server. This can be a descriptive name for easier identification.
Server IP addr	Provide the IP address of the RADIUS or TACACS+ server.
Select server	Set to either RADIUS or TACACS+.
Authentication port	This is an optional parameter for RADIUS servers. If TACACS+ is selected, the port is fixed to TCP port 49.

The screenshot below shows a RADIUS server that has been added to the configuration using the standard authentication port 1813 (UDP).



6.11.4 AAA Authentication

6.11.4.1 *Login Authentication*



Item	Description
Choose a domain	Select the ISP domain.
Login Authentication	Check to activate it.
First – Fourth Method	None: Eliminates the requirement for any authentication method. Local: Uses the local password configured on the device to grant access. Group RADIUS: Uses the list of all RADIUS servers for authentication. Group TACACS+: Uses the list of all TACACS+ servers for authentication. Custom Server Group: Uses authentication of a custom server group.

6.11.4.2 *Enable Authentication*

This page allows the user to add, edit or delete enable authentication list settings (the “default” list cannot be deleted). The line combined to this list will authenticate a user who is issuing the ‘enable’ command by one of the four methods in this list. If the first method fails, the next priority method will be tried to authenticate, and so on.

6.11.4.3 *Dot1x Authentication*

The 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports, unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Note: If you activate this but have not configured any of the authentication methods (i.e., RADIUS) correctly, you will lose access to the Intellinet switch, and you may need to perform a hardware reset in order to re-gain access to the web admin interface. See section 2.4.1 Front Panel.

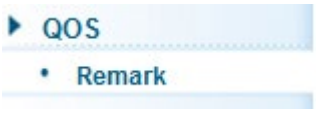
6.12 QoS – Quality of Service

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

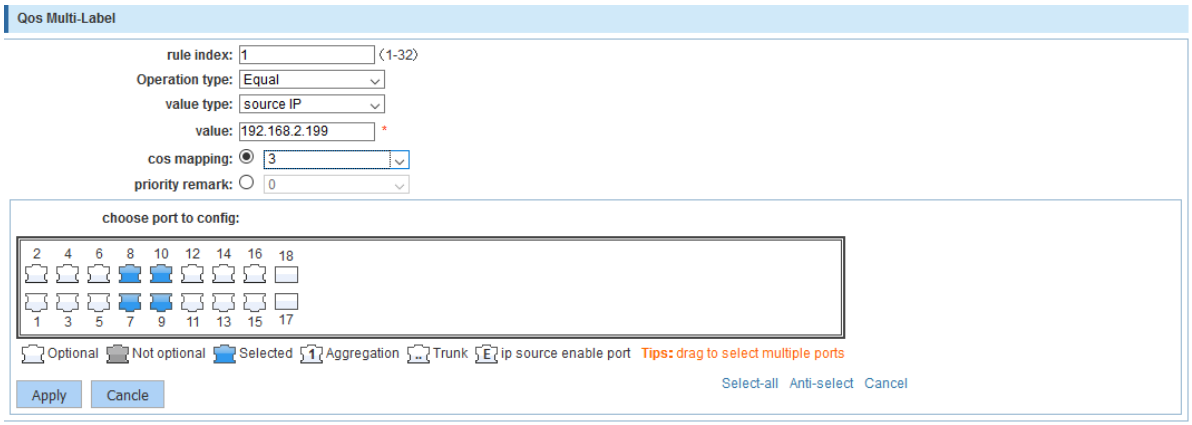
You can use QoS on your system to control a wide variety of network traffic by:

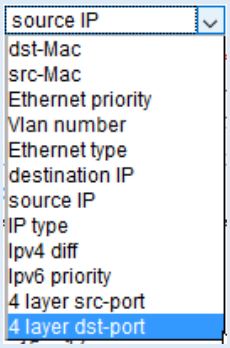
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or Voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

6.12.1 QoS Rules

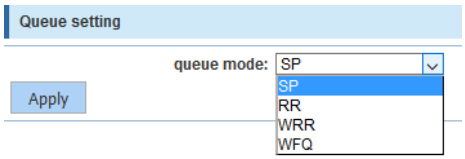


Despite the name “Remark” or “QoS Multi-Label, this section actually allows you to create your Quality of Service rules.



Item	Description
Rule Index	Key in the rule number.
Operation type	Set to “Equal” or “Always match”.
Value type	 This value defines the kind of value you intend to use for the QoS rule.
Value	Key in the value that corresponds to the value type you selected above.
CoS mapping	CoS stands for Class of Service. There are eight values to choose from.
Priority remark	Priority / Description 0 – Routine (HTTP, FTP) 1 – Priority 2 – Immediate (DNS) 3 – Flash (Telnet, SSH, RDP) 4 – Flash Override 5 – Critical (VoIP) 6 – Internetwork Control (Remote router configuration) 7 – Network Control (Firewall, router, switch management) As an alternative to CoS mapping, you can define the priority value here, values 0 – 7.
Choose port to config	Select the port or ports for the QoS rule. Select all ports if you want the ruke to apply to whichever port the devices are connected to.

6.12.2 Queue Config



In this section you define which priority algorithm you wish the Intellinet switch to utilize.

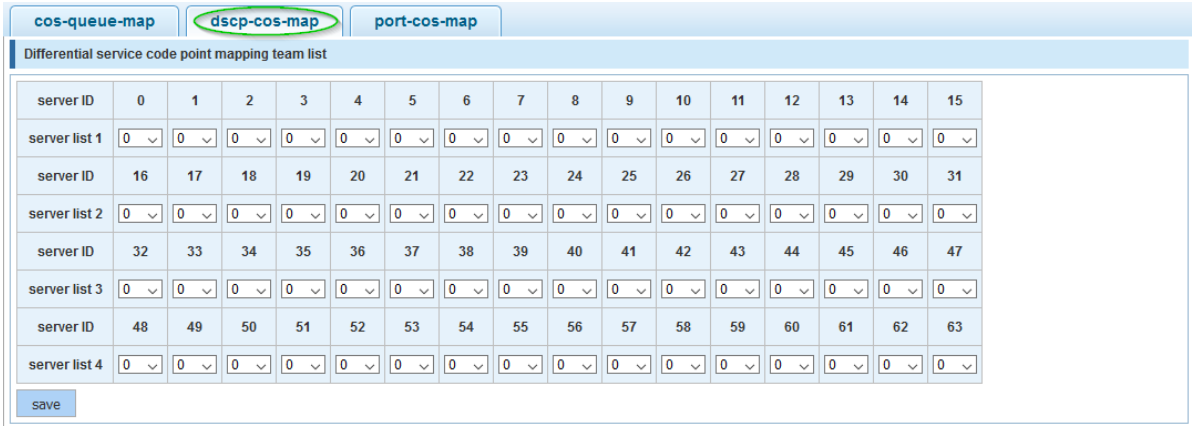
Item	Description
Queue mode	SP = Strict Priority, RR = Round Robin, WRR = Weighted Round Robin and WFQ = Weighted Fair Queuing.

6.12.3 Queue Mapping

6.12.3.1 *CoS-Queue-Map*

This page allows the network administrator to classify CoS settings to traffic queues. The server ID represents the CoS (Class of Server) ID.

6.12.3.2 *DSCP-CoS-Map*



This allows network managers to determine the output queue that is assigned per a specific DSCP field. The DSCP field ID is represented by the server ID, and the QUEUE ID is listed as the server list on the screen.

6.12.3.3 *Port-CoS-Map*

This page allows the network administrator to classify CoS settings to the 18 physical ports on the Intellinet switch. The server ID represents the CoS (Class of Server) ID.

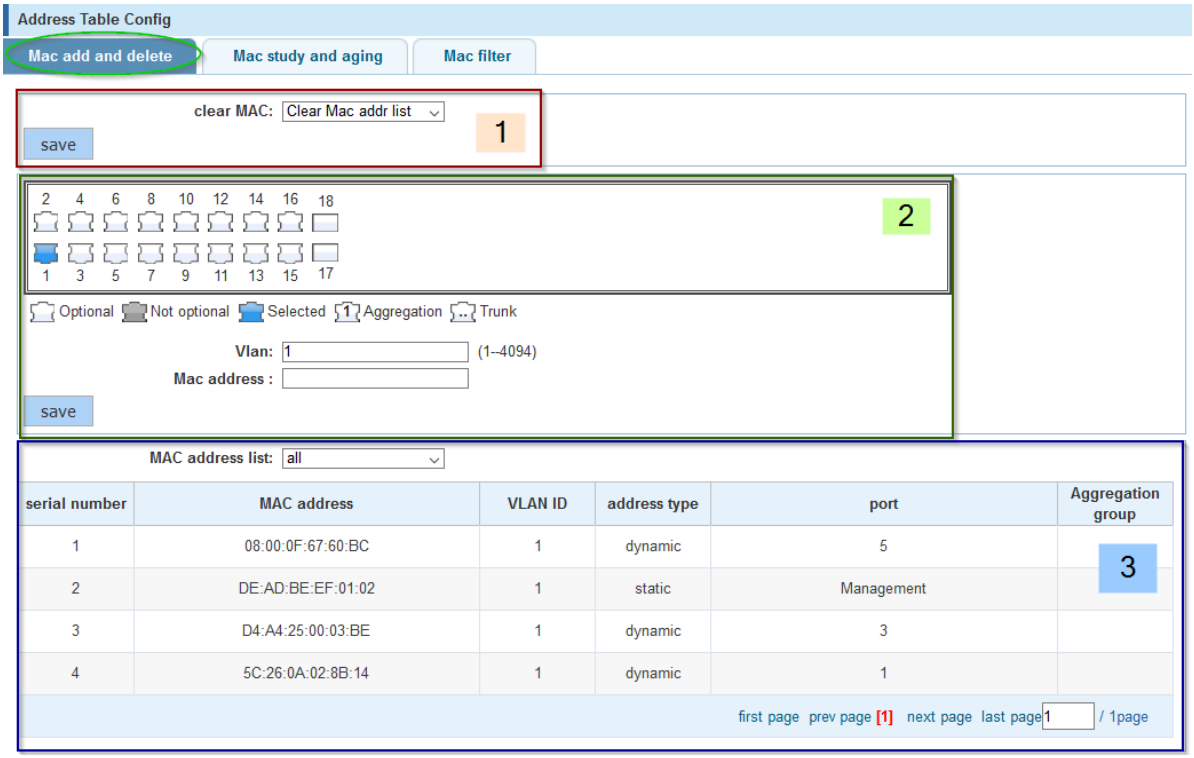
6.13 Address Table

To switch data packets between LAN ports efficiently, the Intellinet switch maintains an address table. When the switch receives a frame, it associates the media access control (MAC) address of the sending network device with the LAN port on which it was received. In doing so, the switch drastically cuts down on unnecessary network traffic, because instead of flooding all LAN ports of the same VLAN with the information, it only sends it to the port where the recipient is connected to.

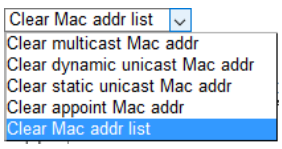
6.13.1 Address Table Config

6.13.1.1 *MAC Add & Delete*

The screen is divided into three sections.



Section 1 ("clear Mac addr list") allows you to clear the MAC address table.

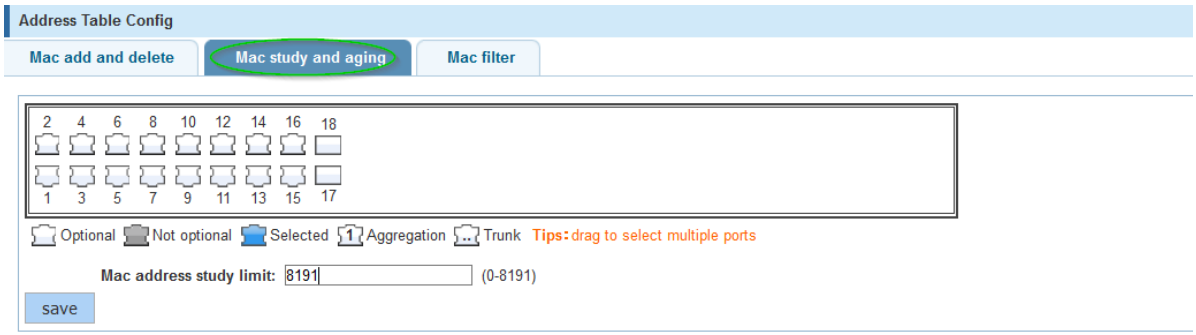


Section 2 can be used to manually enter a VLAN – MAC Address – Port pairing.

Section 3 displays all MAC addresses that are currently in the MAC address table.

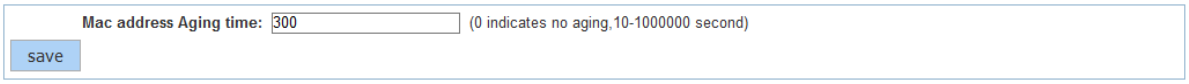
6.13.1.2 *MAC study & aging*

This section allows the network administrator to specify the maximum amount of MAC addresses that can be learnt per port. You can configure a maximum number of secure MAC addresses for each port. The default interface maximum is 8191 addresses. Interface maximums cannot exceed the device maximum, which is also 8191.



Item	Description
Ports	Select one or multiple ports, for which you want to define the MAC addres study limit
MAC address study limit	Key in the maximum MAC address limit for the selected port(s).

The Intellinet switch also provides a mechanism to adjust the aging time for stored MAC addresses. The aging time controls how long the switch keeps storing the MAC address in the MAC address table. Every time a client sends or receives traffic, the aging time for the client's MAC address is reset. If there is no traffic for a MAC address in a time frame that exceeds the time defined in the aging time, the MAC address is removed from the MAC address table. The default aging time is 300 seconds. Setting the value to "0" disables the aging time mechanism, which means that a MAC address that has been learnt once, will be kept in the MAC address table until the switch is reset. But the since the Intellinet switch has only finite space to hold MAC addresses, it is recommended to keep the aging time at, or around the default value.



6.13.1.3 *MAC Filter*

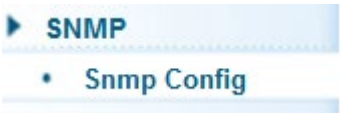
With this feature the network administrator can prevent access to the network for selected MAC addresses and VLAN IDs (1 = default VLAN).

Item	Description
MAC Address	Type in the MAC address that you want to block.
MAC address study limit	Type in the VLAN ID if applicable.

6.14 SNMP

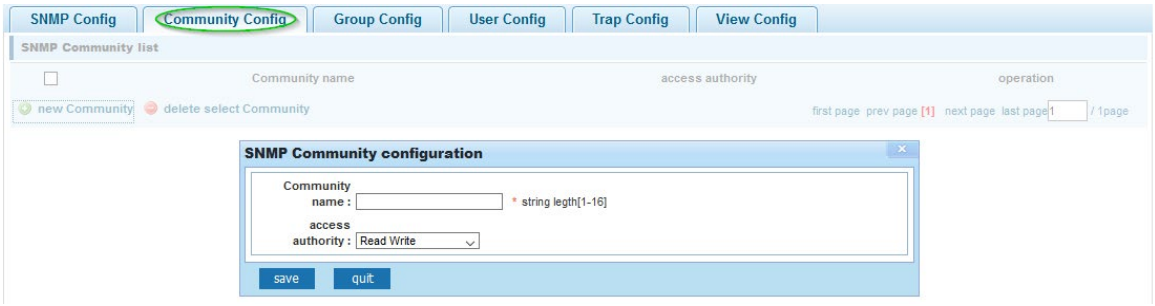
Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

6.14.1 SNMP Config



Activate or deactivate SNMP.

6.14.1.1 *Community Config*



Item	Description
Community name	SNMP Community string. The SNMP read-only community string is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device.
Access authority	Set to read-only or read-write.

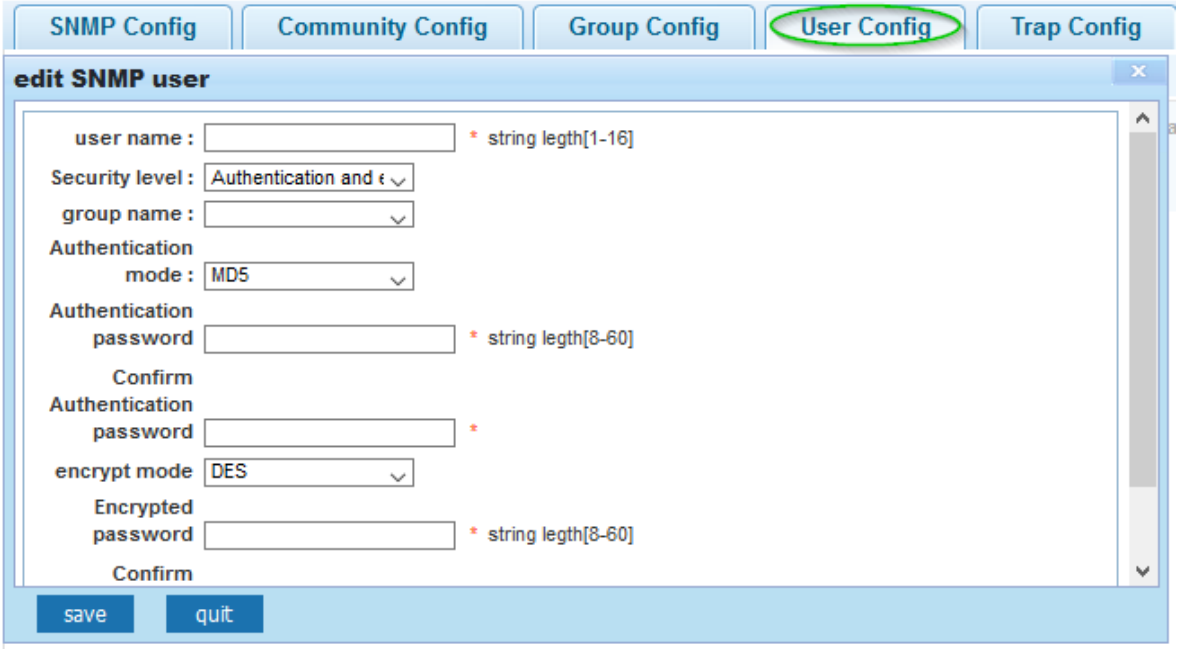
6.14.1.2 *Group Config*

The Intellinet switch uses a view-based access control model that allows the network administrator to configure the access privileges granted to a group.

Item	Description
Group name	Provide a group name.
Security level	Select the desired security level. no Authentication ar no Authentication and no encryption Authentication and no encryption Authentication and encryption
Read view Read and write view Notify view	Assign the desired view (a view must be created first - see SNMP View Config).

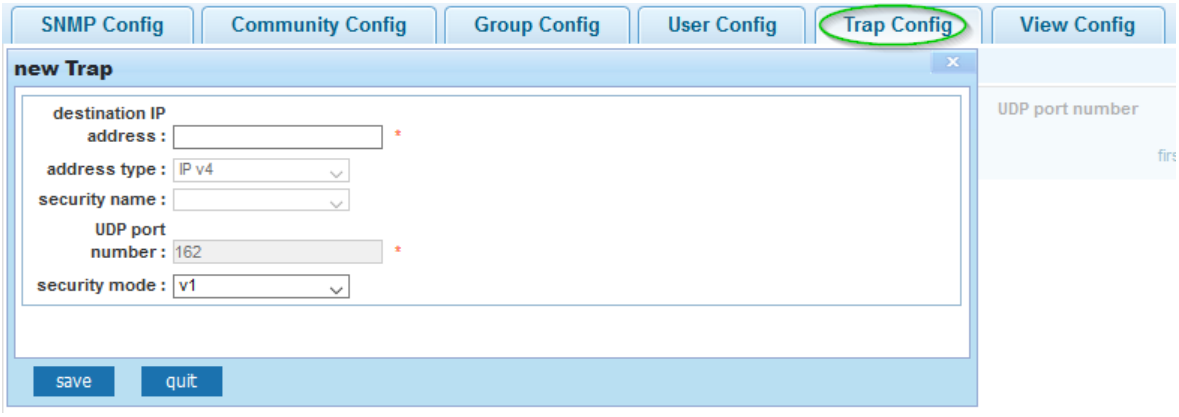
6.14.1.3 *User Config*

This section allows setting up SNMP users and assign them to an SNMP group.



Item	Description
User name	Provide a group name.
Security level	Select the desired security level. no Authentication ar no Authentication and no encryption Authentication and no encryption Authentication and encryption
Group name	Provide a group name.
Authentication mode	Select the hash function of choice. MD5 MD5 SHA
Authentication password	Key in the password.
Encryption mode	Select either AES or DES to encrypt the password.
Encrypted password	Key in the encrypted password.

6.14.1.4 *Trap Config*

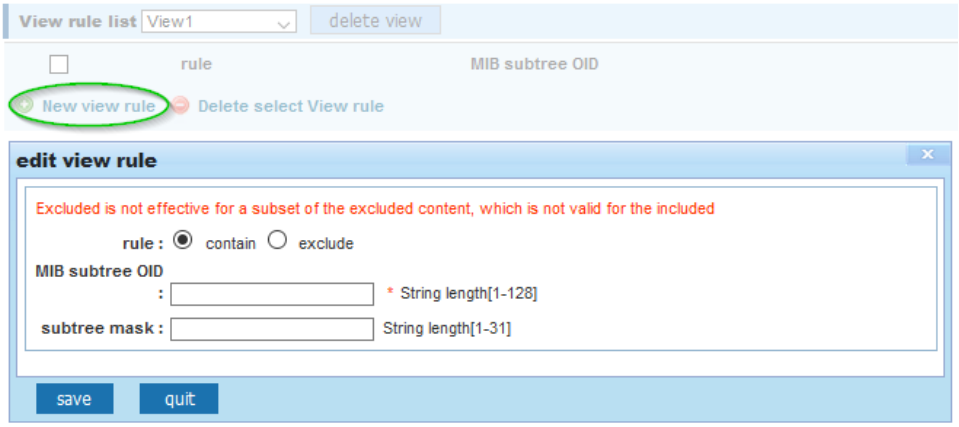


Item	Description
Destination IP Address	The IP address of the SNMP manager (TRAP viewer).
Address type	IPv4 (and perhaps later IPv6 will be supported)
Security name	When using security mode v3, you can select a user from a drop down list. That user was created in the SNMP user config.
UDP port number	Port for Simple Network Management Protocol Trap (SNMPTRAP).
Security mode	Select the security mode (V1, V2 or V3).

6.14.1.5 *View Config*

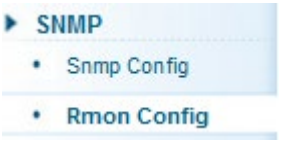
SNMPv3 defines the concept of MIB views in RFC 3415, View-based Access Control Model (VACM) for SNMP. MIB views provide an agent better control over who can access specific branches and objects within its MIB tree. A view consists of a name and a collection of SNMP object identifiers, which are either explicitly included or excluded. Once defined, a view is then assigned to an SNMP group - see SNMP Group Config.

Once a view has been created, you can create a rule for the view.



Item	Description
Rule	Also referred to as the '"Type". Specifies whether to include or exclude the view subtree or family of subtrees from the MIB view.
MIB subtree OID	Enter an OID string for the subtree to include or exclude from the view. OID string is 256 characters in length. For example, the system subtree is specified by the OID string .1.3.6.1.2.1.1.
Subtree mask	Provide the OID mask here.

6.14.2 RMON Config



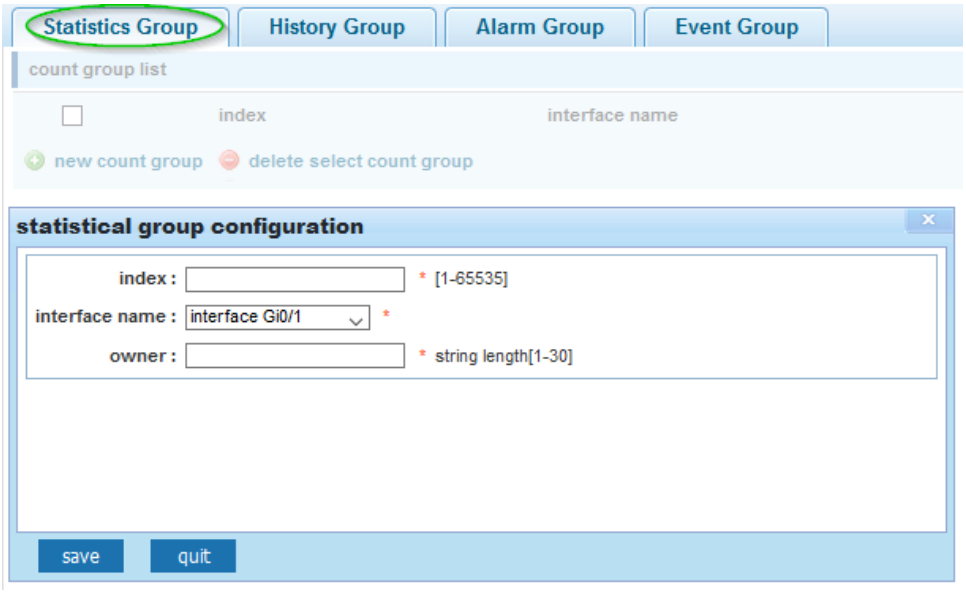
Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch supports the most frequently used group 1, 2, 3 and 9:

- Statistics: Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface.
- History: Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.
- Alarm: Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Event: Determines the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

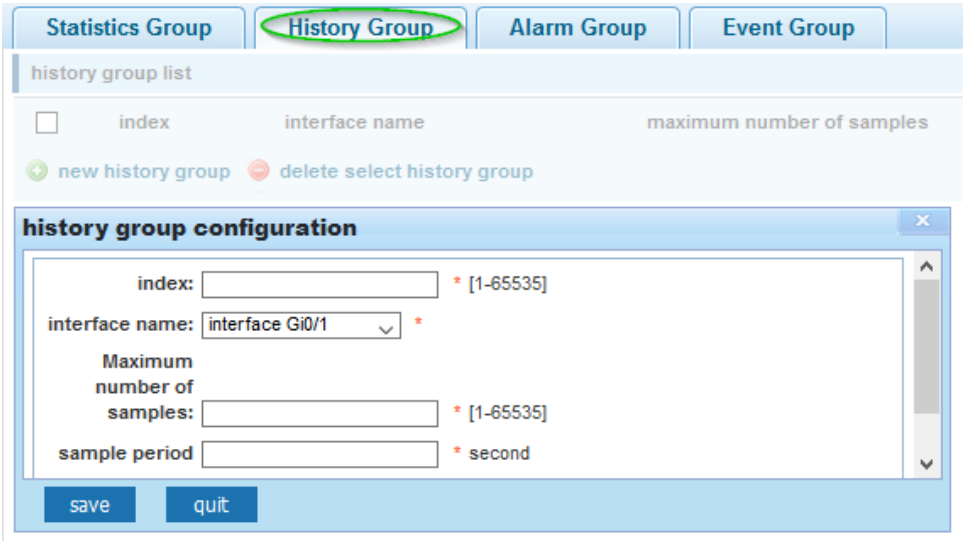
RMON is specified as part of the Management Information Base (MIB) in RFC1757 as an extension of the Simple Network Management Protocol (SNMP).

6.14.2.1 *Statistics Group*



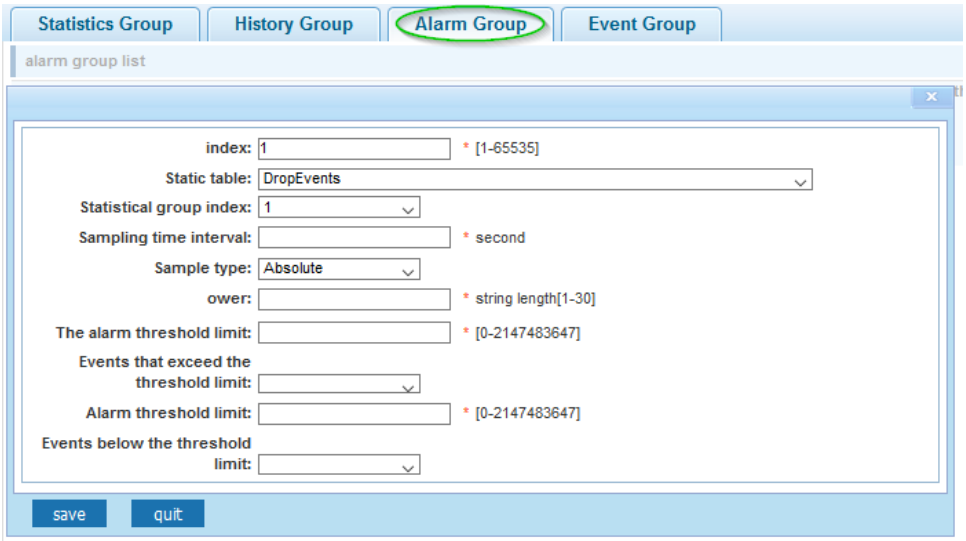
Item	Description
Index	Specify the history table index number.
Interface name	Select one of the eighteen Gigabit port from the drop-down list.
Owner	Optional field that allows the network administrator to enter the name of the owner of the Statistics RMON group.

6.14.2.2 *History Group*



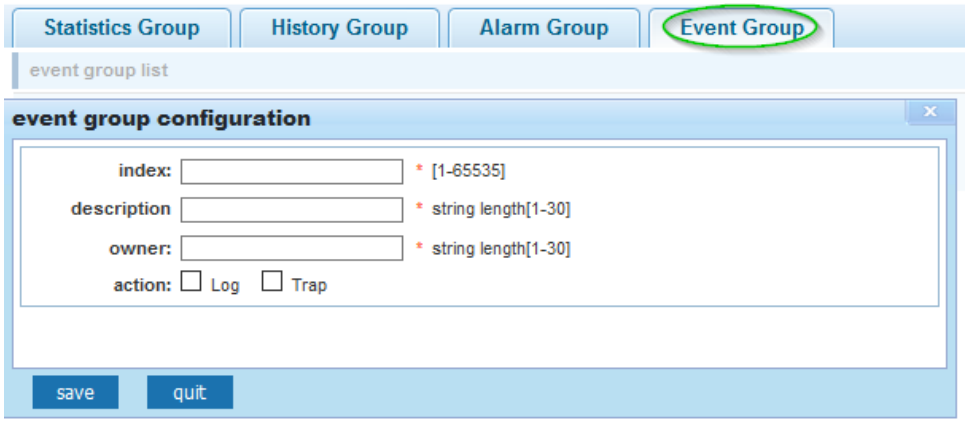
Item	Description
Index	Specify the history table index number.
Interface name	Select one of the eighteen Gigabit port from the drop-down list.
Maximum number of samples	This is the number of samples ("buckets") to keep before they get overwritten.
Sample period	The number of seconds in each polling cycle.

6.14.2.3 *Alarm Group*



Item	Description
Index	Specify the alarm table index number.
Static table	Specify the MIB variable that is monitored by the alarm entry.
Statistical group index	This is the number of samples ("buckets") to keep before they get overwritten.
Sampling time interval	The number of seconds in each polling cycle.
Sample type	This is the method of sampling the selected variable and calculating the value to be compared against the thresholds.
Owner	Optional field that allows the network administrator to enter the name of the owner of the Alarm RMON group.
The alarm threshold limit	This is the rising threshold, a number at which the alarm is triggered. This value ranges between 0 and 2147483647.
Events exceeding threshold	The event number to trigger when the rising threshold exceeds its limit.
Alarm threshold limit	This is the falling threshold, a number at which the alarm is reset. This value ranges between 0 and 2147483647.
Events below threshold limit	The event number to trigger when the falling threshold exceeds its limit.

6.14.2.4 *Event Group*



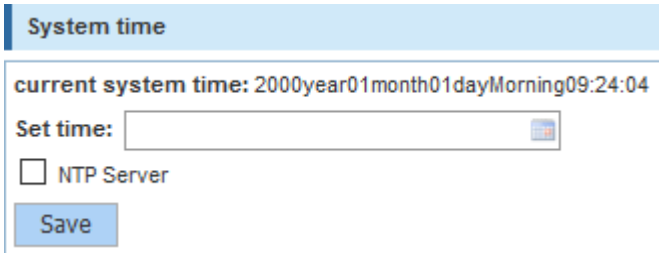
Item	Description
Index	Specify the event table index number.
Description	A descriptive name of the event.
Owner	Optional field that allows the network administrator to enter the name of the owner of the Event RMON group.
Action	Set to either "Log" if you want to generate a log entry, or "Trap" in order generate a trap message.

6.15 SYSTEM

6.15.1 System Config

6.15.1.1 *System Settings*

Item	Description
VLAN	The default VLAN ID of the switch ("1: by default).
IP	The LAN IP address of the switch. The default IP address is "192.168.2.1".
Mask	The default network mask is 255.255.255.0.
Default Gateway	The optional default gateway only is needed when you require Internet access for the Intellinet switch, for example in order to obtain time information from an NTP server.
Jumboframe	Here you can specify the maximum frame size supported by the Intellinet switch. The maximum is 9216 (kB).
DNS Server	The optional DNS server is only needed when you require Internet access for the Intellinet switch, for example in order to obtain time information from an NTP server.
Login timeout	This parameter applies to the web administrator UI. By default, users will be automatically logged out after 30 minutes of inactivity.
IPv6 address	Optional IPv6 address for the Intellinet switch.
Device name	Device name for the Intellinet switch.
Device position, contacts and contact information	Optional additional information you can provide for the Intellinet switch.



Index	Specify the history table index number.
Set time	Click in order to set the time for the Intellinet switch manually.
[ ] NTP Server	Activate this option if you want the Intellinet switch to obtain the system time from a NTP server. For that to work, be sure to provide a proper gateway and DNS server address.

6.15.1.2 *System Restart*

Click "Restart" in order to have the Intellinet switch perform a system restart.

6.15.1.3 *Password*

On this screen you can change the administrator password. The default password is "1234" or the device serial number.

6.15.1.4 *EEE Enable*

Energy-Efficient Ethernet (EEE) is a set of enhancements to the twisted-pair and backplane Ethernet family of computer networking standards that allow for less power consumption during periods of low data activity. The intention was to reduce power consumption by 50% or more, while retaining full compatibility with existing equipment. The Institute of Electrical and Electronics Engineers (IEEE), through the IEEE 802.3az task force developed the standard. EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic.

When a port is powered down for saving power, the outgoing traffic is stored in a buffer until the port is powered up again. Using this technique, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Keep in mind that buffering traffic will give some latency in the traffic.

Should you encounter problems related to EEE, e.g., related to auto negotiation, you can disable EEE support and the Intellinet switch will no longer use it.

6.15.1.5 *SSH Login*

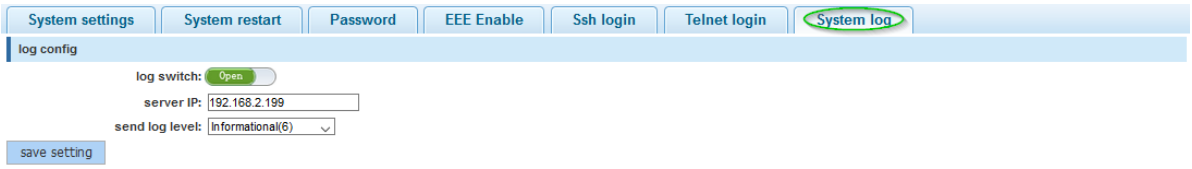
Activate SSH support by setting the SSH CONFIG to "OPEN".

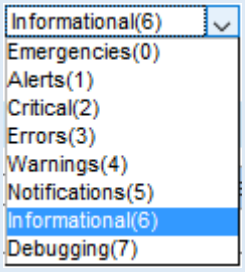
6.15.1.6 *Telnet Login*

Activate Telnet support by setting the TELNET CONFIG to "OPEN".

6.15.1.7 *System Log*

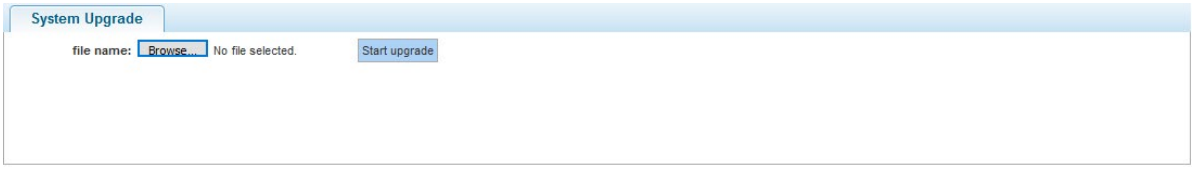
The Intellinet switch has the ability to create a history log of important events. These logs can be stored either in the switches own memory, or on a remote Syslog server. In order to utilize the logging service, you must first enable it.



Index	Specify the history table index number.
Log switch	Select one of the eighteen Gigabit port from the drop-down list.
Server IP	Provide the IP address of the Syslog server. Note that the Syslog server must be set to UDP port 514.
Send log level	Define the amount of detail you wish the Intellinet switch to log. 

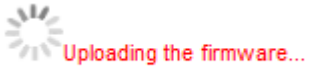
6.15.2 System Update

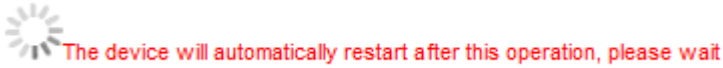
Intellinet may release a new firmware for this switch proving new functions, and perhaps bug fixes. You can install the new firmware on this screen. Should a new firmware be made available, it will be available at http://intellinet-network.com/search?q=561334.



How to install the new firmware:

1. Download the firmware from the web site
2. If the firmware is a compressed file such as RAR, 7Z or ZIP, you need to uncompress the file first, before it can be installed on the intellinet switch.
3. The correct file extension for the firmware is ".bix".
4. Click "Browse" and select the ".bix" file from your computer's HDD
5. Click "Start Upgrade".
6. Confirm your decision by clicking OK. The upgrade will now begin.
7. Hope that there won't be a power outage during the next 3 minutes.



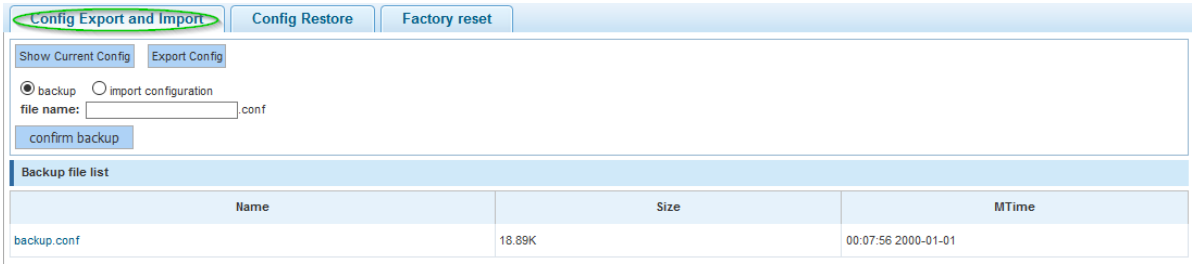


Note that if you still see the message above after 5 minutes, open a new browser window and re-connect to the IP address of the Intellinet switch (default = http://192.168.2.1).

6.15.3 Configuration Management

6.15.3.1 *Config Export and Import*

This function allows to backup and restore the configuration data of the Intellinet switch.

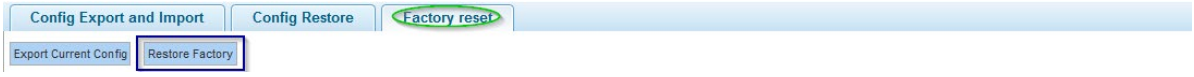


Index	Specify the history table index number.
Show current config	Shows the current switch configuration in a pop-up window.
Export Config	Lets you save the current configuration data to a file on your computer's HDD.
Backup	When a file name is provided (see below), click this button to create a backup of the configuration, which the Intellinet switch is going to keep in its memory. The config restore function provides access to these backups and lets you restore them, delete them, rename them or save them to your computer's HDD.
File name	Filename for backlup, e.g., backup.
Import configuration	In order to upload a previously saved configuration, activate tyhis option, then click on "Browse" and select the correct ".conf" from your computer's HDD. Click the "Import Configuration" button to begin.

6.15.3.2 *Config Restore*

The config restore function provides access to backups that were created previously, and lets you restore them, delete them, rename them or save them to your computer's HDD.

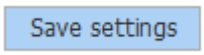
6.15.3.3 *Factory Reset*



This feature allows to restore all settings to the factory default values. If you managed to lock you out from configuring the switch and have lost access to the web admin interface, you can reinstate the factory default settings by pressing the reset button on the front pf the switch for 20 seconds.

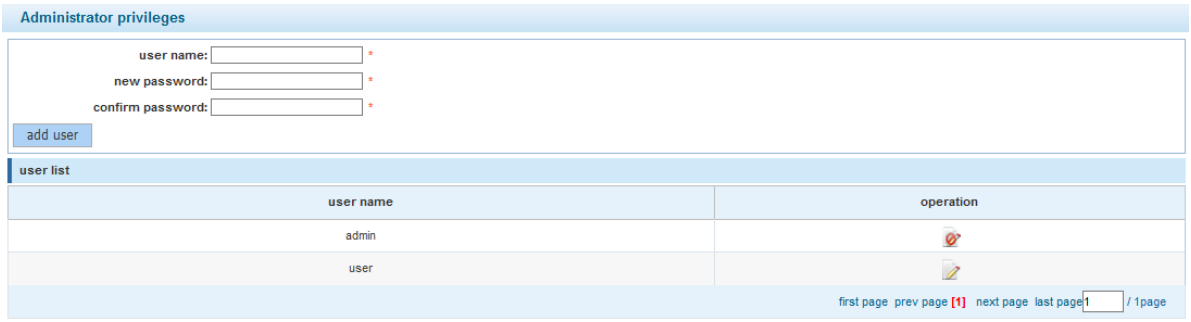
6.15.4 Config Save

The Intellinet 48-Port Gigabit Ethernet Web-Managed Switch provides a myriad of configuration options, many of which are designed for experienced network administrators and aren't easy to configure. It would be a real shame if all the configuration data was lost after a power failure or after the switch was restarted. In order to make the configuration permanent, it needs to be saved.



6.15.5 User Accounts

You can create new user accounts and modify existing ones on this page. A user account that does not have administrator right can only monitor the main status information of the Intellinet switch, but cannot make any changes to the configuration.

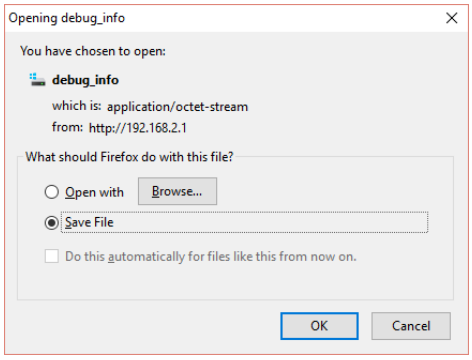


Index	Specify the history table index number.
User name	When creating a new account, type in the new username. If editing you are editing an existing account, the field will be read-only.
New password	Type in the new password.
Confirm new password	Repeat the new password.

6.15.6 Information Collect

Click on the

button create a file that contains the configuration data of the Intellinet switch. A few seconds later you will be asked to open or save the file (or whatever web browser default action for unknown files is in place on your system). This information can be useful when it comes to troubleshooting technical problems.



7 WARRANTY

Deutsch - Garantieinformationen finden Sie hier unter intellinetnetwork.com/warranty.

English - For warranty information, go to intellinetnetwork.com/warranty.

Español - Si desea obtener información sobre la garantía, visite intellinetnetwork.com/warranty.

Français - Pour consulter les informations sur la garantie, rendezvous à l'adresse intellinetnetwork.com/warranty.

Italiano - Per informazioni sulla garanzia, accedere a intellinetnetwork.com/warranty.

Polski - Informacje dotyczące gwarancji znajdują się na stronie intellinetnetwork.com/warranty.

México - Póliza de Garantía Intellinet — Datos del importador y responsable ante el consumidor IC Intracom México, S.A.P.I. de C.V. • Av. Interceptor Poniente # 73, Col. Parque Industrial La Joya, Cuautitlan Izcalli, Estado de México, C.P. 54730, México. • Tel. (55)1500-4500

La presente garantía cubre los siguientes productos contra cualquier defecto de fabricación en sus materiales y mano de obra.

A. Garantizamos cámaras IP y productos con partes móviles por 3 años.

B. Garantizamos los demás productos por 5 años (productos sin partes móviles), bajo las siguientes condiciones:

1. Todos los productos a que se refiere esta garantía, ampara su cambio físico, sin ningún cargo para el consumidor.

2. El comercializador no tiene talleres de servicio, debido a que los productos que se garantizan no cuentan con reparaciones, ni refacciones, ya que su garantía es de cambio físico.

3. La garantía cubre exclusivamente aquellas partes, equipos o sub-ensambles que hayan sido instaladas de fábrica y no incluye en ningún caso el equipo adicional o cualesquiera que hayan sido adicionados al mismo por el usuario o distribuidor.

Para hacer efectiva esta garantía bastará con presentar el producto al distribuidor en el domicilio donde ue adquirido o en el domicilio de IC Intracom México, S.A.P.I. de C.V., junto con los accesorios contenidos n su empaque, acompañado de su póliza debidamente llenada y sellada por la casa vendedora indispensable el sello y fecha de compra) donde lo adquirió, o bien, la factura o ticket de compra original donde se mencione claramente el modelo, numero de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese tilizado en condiciones distintas a las normales; si el producto no ha sido operado conforme a los instructivos de uso; o si el producto ha sido alterado o tratado de ser reparado por el consumidor o terceras personas.

8 COPYRIGHT

Copyright ©2016 IC Intracom. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

9 Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be 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:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

intellinetnetworkcom

© IC Intracom. All rights reserved.

Intellinet is a trademark of IC Intracom, registered in the U.S. and other countries.