

8-PORT GIGABIT WEB-SMART SWITCH

USER MANUAL

Model 561099



FCC Certifications

This Equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.



Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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.

CE Mark Warning

This equipment complies with the requirements relating to the EMC Directive 2004/108/EC and 2014/30/EU, the Low Voltage Directive 2006/95/EC and 2014/35/EU, and the RoHS Directive 2011/65/EU.



Intellinet has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:

All trade names and trademarks are the properties of their respective companies.

Copyright © 2015 Intellinet, All Rights Reserved.

1 Contents

2	Introduction	5
2.1	General Description	5
2.2	Key Features	5
2.3	The Front Panel	6
2.4	The Rear Panel	6
2.5	Hardware Installation	7
2.6	Connect to Web Admin Interface	7
3	System Configuration	8
3.1	Management	8
3.1.1	Switch Information	8
3.1.2	IP Address Settings	9
3.1.3	Port Setting	9
3.1.4	Trunk Group Settings	11
3.1.5	EEE – Energy Efficient Ethernet	12
3.2	Maintenance	13
3.2.1	User Account	13
3.2.2	Firmware Upgrade	14
3.2.3	Config Backup and Restore	16
3.2.4	Reset to Default Config	17
3.2.5	Config Save	18
3.2.6	Reboot	18
3.3	MultiCast	19
3.3.1	IGMP Snooping	19
4	Monitoring	20
4.1	Port Statistics	20
4.2	Diagnostic	21
4.3	Port Mirroring	22
5	VLAN	23
5.1	VLAN Mode Setting	24
5.2	Port Based VLAN	24
5.3	MTU VLAN	26
5.4	802.1Q VLAN	27
5.4.1	802.1Q Static VLAN	27
5.4.2	802.1Q VLAN Port	28
6	QoS	30
6.1	Port-based Priority	30
6.2	Bandwidth Control	32
7	Security	33

7.1	Storm Filter	33
7.2	Loop Prevention	34
7.3	DHCP Snooping	35
8	Appendix A: Changing the IP Address of a Network Adapter	36
8.1	Windows 8	36
8.2	Windows 7 and 10	39
8.3	Windows XP:	40
8.4	Mac OS X	41
9	Warranty	42
10	Copyright	43
11	Federal Communication Commission Interference Statement	44

2 Introduction

2.1 General Description

The device is a high-performance Gigabit Ethernet switch, with all 8 ports capable of 10/100/1000Mbps auto-negotiation operation (NWay) which means the switch could automatically negotiate with the connected partners on the network speed and duplex mode.

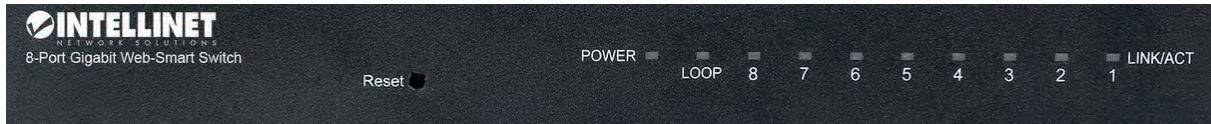
This switch supports the Web GUI to control each port status and bandwidth control by port rate limiting. It's easy to set the VLAN & QoS functions, the VLAN includes MTU VLAN, Port Base VLAN & 802.1Q VLAN. The QoS has 4 priority queues which can set the Storm Filter for Broadcast Storm, Multicast Storm & Unicast Storm. Loop detection and prevention functions are supported for detecting/resolving the cable loopback connection issue more easily. Supports DHCP Snooping function to prevent un-trusted DHCP server installed for easily maintaining network management.

The switch complies with IEEE802.3az Energy Efficient Ethernet to save power consumption, and supports IGMP Snooping to improve traffic performance. Moreover, the rich diagnostic LEDs on the front-panel provide the operating status of individual ports and the whole system.

2.2 Key Features

- 8 x RJ-45 ports for 10/100/1000Mbps connectivity
- All RJ45 ports with Auto-MDIX (auto uplink) support
- Supports 802.3x flow control for full duplex mode and collision-based backpressure for half duplex mode
- Complies with IEEE802.3az Energy Efficient Ethernet
- Supports EEE enable and disable
- Supports IEEE802.3x Flow Control
- Supports storm filter (Broadcast, Multicast, Unicast)
- The QoS supports 802.1p QoS and port rate limiting
- The VLAN includes MTU, Port-based & 802.1Q Tag Based
- Supports 4 groups of port-based VLAN
- Provides port trunk, one group with two member ports
- Provides port mirroring
- Supports IGMP snooping v1/v2/v3
- Supports loop detection and prevention
- Provides cable testing function
- Supports DHCP client
- Supports DHCP snooping
- Firmware update via HTTP and TFTP
- Supports configuration backup & restore
- Supports reset to factory default button

2.3 The Front Panel



LEDs Definition

This device provides extensive LEDs to show the activities on power, system and ports.

See the following description for your reference:

LED	Status	Operation
POWER	Steady Green	The device is powered on.
	Off	The device is powered off.
LOOP	Steady Red	The device has detected a loop on the network.
	Off	No loop has been detected.
Link/ACT	Steady Green	A link has been established to the device connected to this port..
	Blinking Green	Data is transmitted over this port.
	Off	The port is not connected to an active RJ45 Ethernet device.

The Reset Button

Reset the switch to its factory default configuration via the RESET button. Press the RESET button for more than five seconds to enable reset to default function. The switch automatically reboots and reloads its factory configuration file.

2.4 The Rear Panel

The following figure shows the rear panel of the switch:



Power connector and RJ45 Ethernet ports are located on the rear panel of the 8-Port Gigabit Web-Smart Switch. Standard Cat5e or Cat6 RJ45 Ethernet cable is supported, including straight-through and crossover variants.

2.5 Hardware Installation

Desktop Installation

Place the switch on a flat surface. Ensure adequate ventilation space around the switch for dissipating heat and air. Properly connect the device to a power outlet using the included power cable, and it will automatically initialize and the power LED will light up.

Installing Network Cables

To make a valid connection and obtain the optimal performance, an appropriate network cable that corresponds to different transmitting/receiving speeds is required. To choose a suitable cable, please refer to the following table.

Media	Speed	Wiring
Network Media (Cable)	10 Mbps	10Base-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100 Mbps	100Base-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	1000 Mbps	1000Base-T: UTP category 5e, 6 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)

2.6 Connect to Web Admin Interface

In order to configure the smart features of the Intellinet 8-Port Gigabit Web-Smart Switch, you need to set the IP address of your computer's network adapter to a value of 192.168.2.xxx where xxx must not be equal to 1. Refer to Appendix A for details.

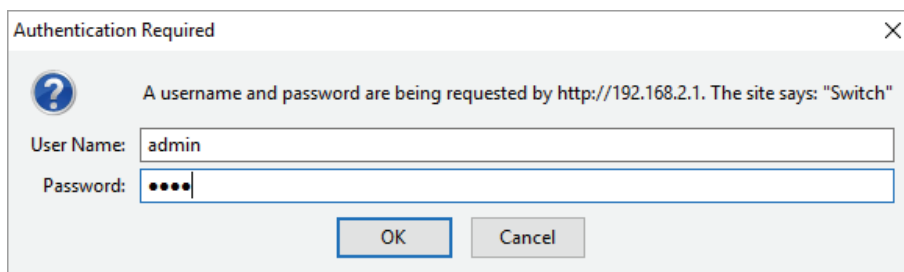
The default IP of the Intellinet 8-Port Gigabit Web-Smart Switch is 192.168.2.1. Open "http://192.168.2.1" in your web browser.



The login screen appears.

User Name: 'admin'

Password: '1234'

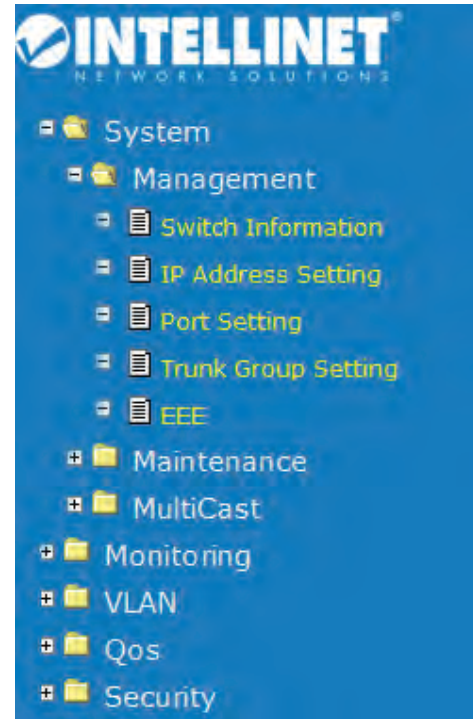


3 System Configuration

3.1 Management

3.1.1 Switch Information

This page displays some core information about the Intellinet 8-Port Gigabit Web-Smart Switch. The information is read-only, except for the switch name, which you can edit.

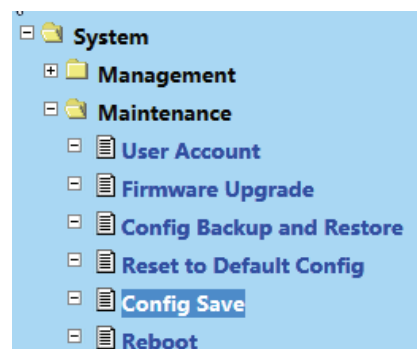


Switch Information	
Switch Name	Intellinet 561099
MAC Address	00:08:54:72:AD:A2
Firmware Version	V1.0.2_1123
DHCP client	Disable
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Apply	



In order to save any changes you make to the programming of the Intellinet 8-Port Gigabit Web-Smart Switch, you are going to have to click on  **Config Save**.

The configuration has been saved successfully.



3.1.2 IP Address Settings

DHCP client
IP Address
Subnet Mask
Gateway

Disable ▾

192.168.2.1

255.255.255.0

192.168.2.254

Apply

LABEL	DESCRIPTION
DHCP Client	Enable or disable the DHCP Client function. If this is enabled, the Intellinet switch receives its IP settings (IP Address, Subnet Mask and Gateway) from a DHCP server in your LAN, i.e. a router. If set to 'disable', then you must provide the IP information yourself and enter them into the field below.
IP Address	System IP address of the switch. The default value 192.168.2.1.
Subnet Mask	Subnet mask of the switch. The default value is 255.255.255.0.
Gateway	Gateway IP address of the switch.
Apply	Click Apply to save and activate the settings.

3.1.3 Port Setting

On this page you can control some basic parameters for the RJ45 ports on the Intellinet 8-Port Gigabit Web-Smart Switch.

Port Setting

Port	State	Speed/Duplex	Flow Control
Port 1			
Port 2			
Port 3			
Port 4	Enable ▾	Auto ▾	Off ▾
Port 5			
Port 6			

Note: The flow control function can be configured as ON and takes effect only when one port's Config mode of Speed/Duplex is Auto and its Actual mode is 1000MF/100MF/10MF

Apply

LABEL	DESCRIPTION
Port	Select the port which you wish to configure from the list box.
State	Allows you to Enable/Disable the port.
Speed/Duplex	Auto: Enables maximum Gigabit full duplex performance 10M/Half: 10 Mbps, half-duplex 10M/Full: 10 Mbps, full-duplex 100M/Half: 100 Mbps, half-duplex 100M/Full: 100 Mbps, full-duplex
Flow Control	Enable or disable the flow control ability of the selected ports.
Apply	Click Apply to save the settings and activate them.

Port	State	Speed/Duplex		Flow Control	
		Config	Actual	Config	Actual
Port 1	Enable	Auto	Link Down	On	Off
Port 2	Enable	Auto	Link Down	On	Off
Port 3	Enable	Auto	Link Down	On	Off
Port 4	Enable	Auto	Link Down	On	Off
Port 5	Enable	Auto	Link Down	On	Off
Port 6	Enable	Auto	Link Down	On	Off
Port 7	Enable	Auto	Link Down	On	Off
Port 8	Enable	Auto	1000Full	On	On

Port	Displays the port number.
State	Displays the actual state of the port.
Speed/Duplex	Config: Displays the configuration of link speed and duplex mode for the port. Actual: Displays the actual working state of the port.
Flow Control	Config: Displays the configuration of the flow control for the port. Actual: Displays the actual working state of the port.



Note:

The switch can't be managed through a disabled port. Be sure not to disable the port through which you are connecting to the switch.

3.1.4 Trunk Group Settings

To create a link between the Intellinet 8-Port Gigabit Web-Smart Switch, you normally simply connect an RJ45 Ethernet cable to a port on a different switch. If that is also a Gigabit switch, this connection between the two switches would provide a bandwidth of 1 Gbps. In order to increase the bandwidth, you can set up a so called trunking group, which takes two physical ports and combines them to one logic port, doubling the bandwidth to 2 Gbps.

Trunk Group Setting

Group ID	Ports
Trunk	Port 1 Port 2 Port 3 Port 4

Note: 1.Trunk Group Setting can only support port 1 - 4.
2.Trunk Group Setting can be supported only if Loop Prevention/Loop Detection is disabled.

Add / Modify

1. Select any two ports of ports one to four.
2. Click Add/Modify to create the trunk group



Note:

When using trunk groups, the following restrictions apply:

- You may only create one trunking group.
- Only two ports can form a trunking group, and only ports 1 – 4 can be a member of a trunking group.
- All member ports of a trunk group must have identical port & QoS settings.
- All member ports of a trunk group must have the same port-based priority.
- All member ports of a trunk group must have the same 802.1Q VLAN port setting.
- All member ports of a trunk group must have the same storm filter rate.
- All member ports of a trunk group must have the same frame type.
- The Gigabit switch on the opposite end must also be configured with a trunking group consisting of two ports.

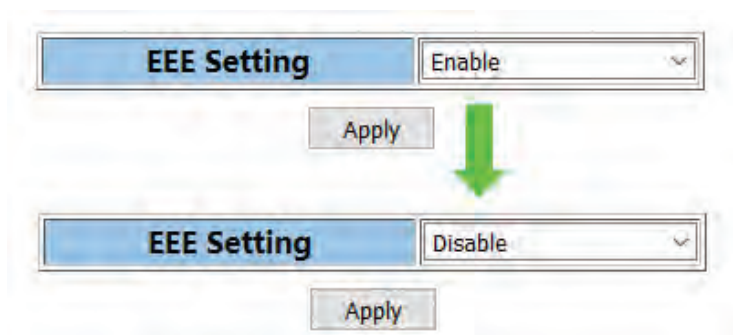
3.1.5 EEE – Energy Efficient Ethernet

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 add some latency in the traffic.

If EEE is not desired in your network environment, you can disable this feature on this screen.



3.2 Maintenance

3.2.1 User Account

On this screen you can change the user name and password required to access the web administrator configuration menu.

User Account Setting

New Username	admin
New Password	
Retype Password	
Apply	

Enter a new username and password, then click Apply. You will then have to enter the new username and password in order to log back into the configuration.

Authentication Required


A username and password are being requested by http://192.168.2.1. The site says: "Switch"

User Name:

Password:



Note:

Only digits and regular alpha numeric characters can be used for creating the user name and password. Do not use any special characters. The length of the user name should not be more than 20 characters and the password should not be longer than 17 characters.

3.2.2 Firmware Upgrade

If a new firmware needs to be installed, you can use this screen to do it. You can install a new firmware image (file) using TFTP, or HTTP. In order to begin the process, you must first enter the so-called loader mode.

Firmware Upgrade
Enter loader mode to upgrade firmware. After entering loader mode, configuration will be saved.

Enter Loader Mode

Enter Loader Mode?

OK
Cancel

After you click OK, you will see a new menu on the left side of the screen. This menu provides access to the TFTP and HTTP method of updating the firmware.

Firmware Upgrade

TFTP Firmware Upgrade
HTTP Firmware Upgrade
Reboot

TFTP

To install the upgrade via TFTP, a TFTP server must be configured to accept connections from the Intellinet switch. Provide the IP address of the TFTP server along with the correct file name that you wish to install.

TFTP Firmware Upgrade

TFTP Server IP Address
192.168.1.2

Image File Name
561099_newfirmwareimage.bin

Download Image

Enter the Image File Name and click Download Image, then a message will pop up.

Message from webpage


It takes several seconds for FW downloading process. After firmware downloading is complete, the switch automatically reboots. This briefly disrupts network traffic through the switch. Continue?

OK
Cancel

Click OK and allow the procedure to complete. The switch will perform a restart at the end of the firmware upgrade procedure.

Firmware Upgrade Status

Do not disconnect the link or power down the switch during firmware upgrade.
Please wait 14 seconds...

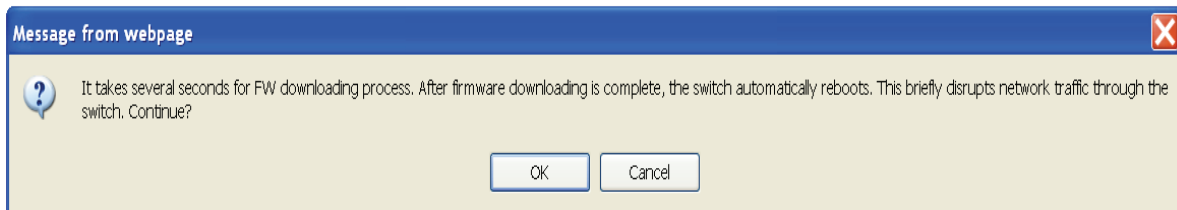
HTTP

In order to install the upgrade, select the appropriate upgrade type, then click on , select the file from your local HDD. Then press to begin.

HTTP Firmware Upgrade

561099_runtime_20151123.bin

Click Upgrade, then a message will pop up.



Click OK and allow the procedure to complete. The switch will perform a restart at the end of the firmware upgrade procedure.

Reboot

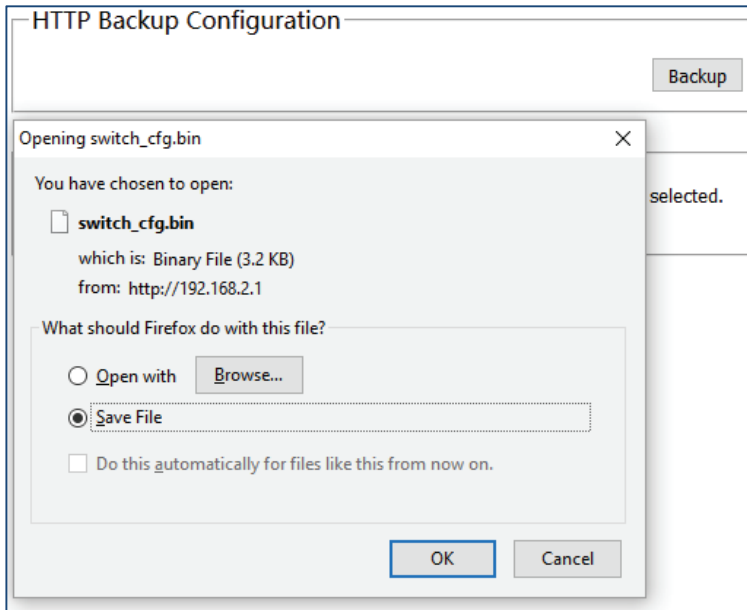
Please wait 17 seconds to reboot...

In order to leave the loader mode and return to the standard operation mode, click on 'Reboot.'

3.2.3 Config Backup and Restore

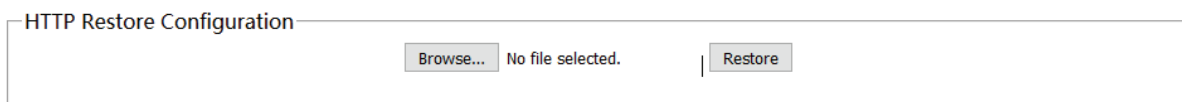
On this page you can save the entire configuration of the Intellinet 8-Port Gigabit Web-Smart Switch to a file, so you can re-load (restore) it at a later time.

Click on **Backup** to begin. Then select **Save File** and click **OK**.
Then select the location where you wish to save the file, and click **Save**.



In order to restore a previously saved configuration, you have to select the configuration file using the

Browse... button, and then click on **Restore**.

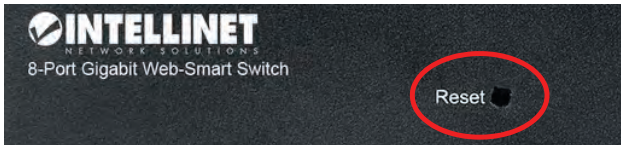


3.2.4 Reset to Default Config

There are two ways to reset the Intellinet switch back to its factory default settings.

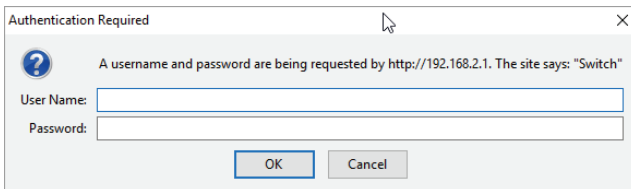
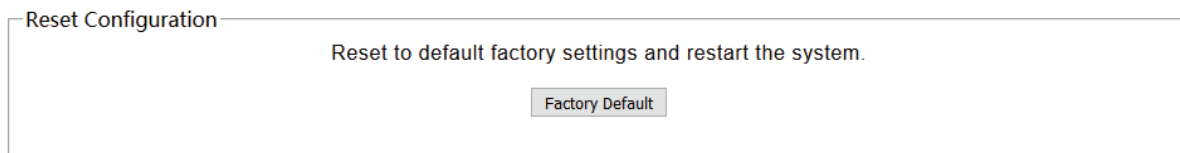
Via Reset Button

Press the reset button for at least 10 seconds while the switch is operation in order to trigger the factory default reset.



Via Web Administrator Menu

Click on **Factory Default**, then provide administrator credentials and click 'OK' to begin.



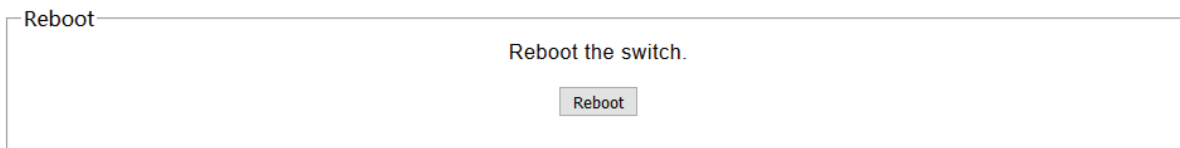
3.2.5 Config Save

In order to save any changes you make to the programming of the Intellinet Gigabit switch, you are going to have to click on  **Config Save**. Once done, the message below confirms that all settings have been saved.

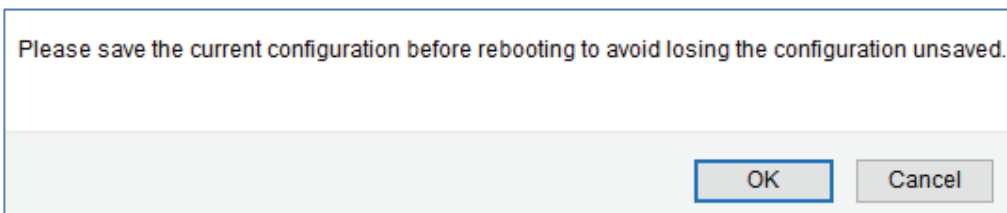


3.2.6 Reboot

If you need to reboot the Intellinet switch from a remote location, this is the way to do it. When the reboot is triggered, the switch won't be accessible and operational for about 60 seconds.



The following message will remind you that any settings not yet saved into the configuration (see previous section) will be lost, so be sure to click on  **Config Save** first.



3.3 MultiCast

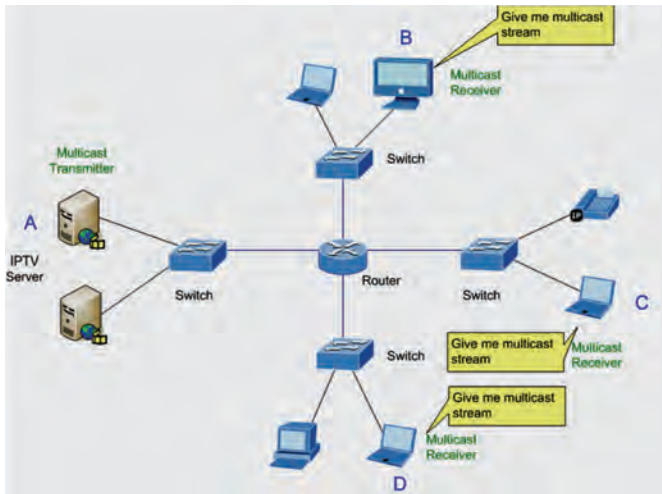
3.3.1 IGMP Snooping

The Internet Group Management Protocol (IGMP) lets hosts and routers share information about multicast group memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for future processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The Internet Group Management Protocol (IGMP) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

Multicast Service



You can enable or disable IGMP Snooping on this screen.

IGMP Snooping

IGMP snooping

Disable

Apply

4 Monitoring

4.1 Port Statistics

These pages provides statistical data about the network ports of the Intellinet switch.

Port Statistics

Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 1	Enabled	Link Down	0	0	0	0
Port 2	Enabled	Link Down	0	0	0	0
Port 3	Enabled	Link Down	0	0	0	0
Port 4	Enabled	Link Down	0	0	0	0
Port 5	Enabled	Link Up	432	0	431	0
Port 6	Enabled	Link Down	0	0	0	0
Port 7	Enabled	Link Down	0	0	0	0
Port 8	Enabled	Link Down	0	0	0	0

LABEL	DESCRIPTION
Port	Displays the port number of the switch.
State	Displays whether the port is enabled or disabled.
Link Status	Displays the link state of the port.
TxGoodPkt	Displays the number of good packets transmitted on the port.
TxBadPkt	Displays the number of error packets transmitted on the port.
RxGoodPkt	Displays the number of good packets received on the port.
RxBadPkt	Displays the number of error packets received on the port.
Clear	Click to reset the port statistic data.

4.2 Diagnostic

With this page it is possible to test all connected cables.

Cable Diagnostic

Check	Port	Test Result	Cable Fault Distance
☐	Port 1	-	-
☐	Port 2	-	-
☐	Port 3	-	-
☐	Port 4	-	-
☐	Port 5	-	-
☐	Port 6	-	-
☐	Port 7	-	-
☒	Port 8	Normal	PairA:2(M), PairB:2(M), PairC:2(M), PairD:2(M)

Apply

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Check	Click the checkbox to select the port to be diagnosed.
Port	Displays the port number of the switch.
Test Result	Open: The cable is broken or no cable connection. Normal: The cable connection is good.
Cable Fault Distance	Displays the distance from the port where the cable error occurred.
Apply	Click Apply to save the settings and activate them immediately.

4.3 Port Mirroring

Network engineers or administrators use port mirroring to analyze and debug data or diagnose errors on a network. It helps administrators keep a close eye on network performance and alerts them when problems occur. It can be used to mirror either inbound or outbound traffic (or both) on single or multiple interfaces. Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.

Port Mirroring

Mirror Direction

Disable ▾

Mirroring Port

Port 1 ▾

Mirrored Port List

Port 1 ▾

Apply

Mirror Direction

Both

Mirroring Port

8

Mirrored Port List

2

Delete

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Mirror Direction	Rx: Received traffic Tx: Transmitted traffic Both: Transmitted and received traffic
Mirroring Port	Define which port will output the mirrored traffic. This is the port to which you connect your monitoring station.
Mirrored Port List	Define which of the 8 ports you wish to mirror the traffic for. Note that the mirrored port cannot be the same as the mirroring port.
Apply	Click Apply to create the new port mirroring rule.
Delete	Click Delete to remove the port mirror rule.



Note:

You can only create one port mirroring rule at a time.

You can only mirror the contents from one port to one other port, but not mirror the contents of multiple ports.

5 VLAN

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily. VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated. The Intellinet 8-Port Gigabit Web-Smart Switch supports three types of VLANs.

Port-based VLANs

Port-based VLAN limits traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department. On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

IEEE 802.1Q VLANs

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant). VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources. VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

Tagging - The act of putting 802.1Q VLAN information into the header of a packet.

Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

MTU multi-tenant unit VLAN

This is a one-click solution which generates a VLAN setup where one port is accessible from all other ports, but the other seven ports are isolated from one another. A possible application could be an apartment building where up to 7 families share an Internet connection. The Internet Router or Gateway is connected to port 1 whereas the other 7 families are connected to ports 2 – 8.



5.1 VLAN Mode Setting

Select the VLAN mode you wish to use.

VLAN Mode Setting

VLAN Mode Setting

Port based VLAN

802.1Q VLAN

Port based VLAN

MTU VLAN

5.2 Port Based VLAN

Allows you to assign ports to virtual networks. Data from a port that is a member of a VLAN group is restricted to other members of that VLAN group. This feature provides an easy way to partition a network into private sub networks.

VLAN ID	(1-4)			VLAN Name					
Port	Select All	1	2	3	4	5	6	7	8
Not Member	All	☒	☒	☒	☒	☒	☒	☒	☒
Member	All	☐	☐	☐	☐	☐	☐	☐	☐

Apply

VLAN ID	VLAN Name	Member Ports	Delete
1	Default_VLAN	1-8	☐

Delete

Select All

The following table describes the related labels in this screen.

LABEL	DESCRIPTION
VLAN ID	Enter the ID number of VLAN.
VLAN Name	Optional name for the VLAN.
Port	Displays the port number of the switch
Select All	Click to quickly select all ports at once.
Not Member	Port(s) not member(s) of the VLAN group.
Member	Port(s) that are member(s) of the VLAN group.
Apply	Click Apply to save the settings.
Port-based VLAN Table	
VLAN ID	Displays the ID number of VLAN.
VLAN Name	Displays the name of VLAN.
Member Ports	Displays the port member in the VLAN.
Delete	Click Delete to remove the VLAN ID you selected before.
Select ALL	This helps to select all VLAN IDs to be deleted at one time.



Note:

To ensure the normal communication of the factory switch, the default VLAN of all ports is set to VLAN1. VLAN 1 cannot be deleted. You can only set the valid VLAN ID between figure 1 to 4.

5.3 MTU VLAN

If the VLAN mode MTU is activated, you can configure the settings on this page. There isn't really much to do except for clicking the apply button. That's because MTU VLAN by default isolates ports 2 – 8 and only allows access to the shared port 1.

VLAN ID	1	2	3	4	5	6	7	8
1	☒	☒	☐	☐	☐	☐	☐	☐
2	☒	☐	☒	☐	☐	☐	☐	☐
3	☒	☐	☐	☒	☐	☐	☐	☐
4	☒	☐	☐	☐	☒	☐	☐	☐
5	☒	☐	☐	☐	☐	☒	☐	☐
6	☒	☐	☐	☐	☐	☐	☒	☐
7	☒	☐	☐	☐	☐	☐	☐	☒

Apply

Once you click

Apply

, the new settings will show on the configuration screen:

VLAN ID	VLAN Name	Member Ports
1	Vlan	1-2
2	Vlan	1,3
3	Vlan	1,4
4	Vlan	1,5
5	Vlan	1,6
6	Vlan	1,7
7	Vlan	1,8

Notice how port 1 is shared among all other ports. In this setup for example, port 8 can communicate with port 1, but not with ports 2 – 7.

5.4 802.1Q VLAN

Allows you to create virtual networks using 802.1Q. When using 802.1Q VLAN, you configure ports to be a part of a VLAN group. When a port receives data tagged for a specific VLAN group, the data is discarded unless the port is a member of the VLAN group. This technique is useful for communicating with devices outside of your local network as well as still receiving data from other ports not in your VLAN group. It requires that you know the VLAN group IDs used.

5.4.1 802.1Q Static VLAN

On this page the user can configure the 802.1Q Static VLAN feature and the related settings.

VLAN ID		(1-4094)	VLAN Name						
Port	Select All	1	2	3	4	5	6	7	8
Untagged	All	☐	☐	☐	☐	☐	☐	☐	☐
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☒	☒	☒	☒	☒	☒	☒	☒
Apply									

LABEL	DESCRIPTION
VLAN ID	Enter the ID number of VLAN. Valid values are 1 to 4094.
VLAN Name	Optional name for the VLAN.
Port	Displays the port number of the switch.
Select All	Click to quickly select all ports at once.
Untagged	Configure the egress rule of the traffic on the port as untagged. The switch drops the tag header before forwarding the packet.
Tagged	Configure the egress rule of the traffic on the port as tagged. The switch adds the tag header before forwarding the packet.
Not Member	Port(s) not member(s) of the VLAN group.
Apply	Click Apply to activate the settings.



Note:

The default VLAN (VID = 1) cannot be removed but you can set to untagged/tagged and modify the member ports.

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1	Default_VLAN	1-8	-	1-8	☐
Delete Select All					

LABEL	DESCRIPTION
VLAN ID	Displays the ID number of the VLAN.
VLAN Name	Displays the name of the VLAN.
Member Ports	Displays the member ports of the VLAN.
Tagged Ports	Displays the tagged member ports of the VLAN.
Untagged Ports	Displays the untagged member ports of the VLAN.
Delete	Click Delete to remove the selected VLAN ID.
Select ALL	Click to quickly select all ports at once.

5.4.2 802.1Q VLAN Port

This page shows VLAN port information. The user can assign a PVID number, and the accepted frame type for each port.

Port	PVID	Accepted Frame Type
Port 1 ^ Port 2 Port 3 Port 4 Port 5 Port 6 v		All v
Apply		

Port	PVID	Accepted Frame Type
Port 1	1	All
Port 2	1	All
Port 3	1	All
Port 4	1	All
Port 5	1	All
Port 6	1	All
Port 7	1	All
Port 8	1	All

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the port(s) you wish to configure.
PVID	PVID number for the ports. It can range from 1 to 4094. When adding the tag header to the received untagged packet, the switch will automatically use this PVID value as the VLAN ID of the added tag.
Accepted Frame Type	Select All/Tag-only/Untag-only from the drop-down list.
Apply	Click Apply to save the settings.
802.1Q VLAN Port Table	
Port	Displays the port number.
PVID	Displays the PVID number of the port.
Accepted Frame Type	Displays the accepted frame type of the port.

6 QoS

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.

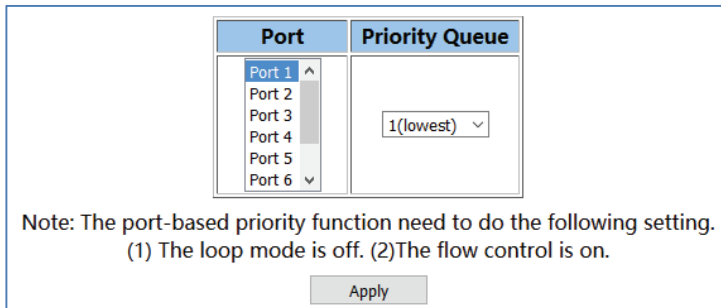
QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

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.

6.1 Port-based Priority

Port-based priority QoS allows you to assign a priority level to each of the 8 ports. The priority levels are: lowest, medium, normal, and highest. By default, all ports are set to priority group 1 (lowest).



Note: The port-based priority function need to do the following setting.
(1) The loop mode is off. (2)The flow control is on.

Apply

Select the port from the left, then choose a priority level from the drop down list on the right, and then click 'Apply' to save the priority level for the port.

LABEL	DESCRIPTION
Port	Select the desired port for configuration. Hold down CTRL to select multiple ports at once.
Priority Queue	Specify the priority queue for that port. The priorities are labeled as 1~4. The higher the value, the higher the priority.

Port	Priority Queue
Port 1	1
Port 2	1
Port 3	1
Port 4	1
Port 5	1
Port 6	1
Port 7	3
Port 8	4

Example Setup

The example above could be used on the following scenario:

1. A Voice over IP phone is connected to port 8. It has the highest priority.
2. A media streaming device such as a smart TV, FireTV, Android TV box, Apple TV or Kodi, is connected to port 7. Only VoIP traffic for port 8 has higher priority.
3. All other devices have the lowest priority.



Note:

The default priority queue for all ports is 1.

- Lowest Priority (background data)
- Normal Priority (business-critical data, email, internet, etc)
- Medium Priority (stream multimedia, etc)
- Highest Priority (interactive voice, video, and delay sensitive data)

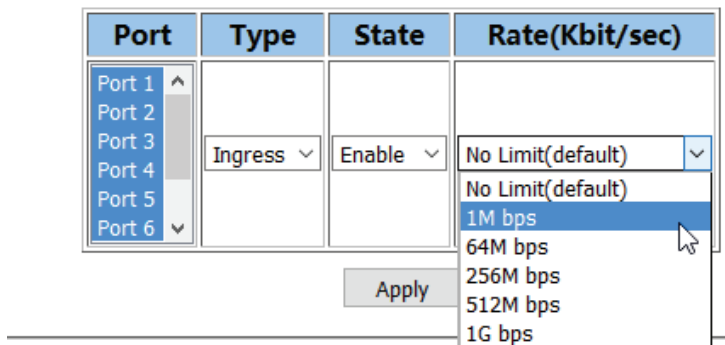
In order to use port-based priority QoS, you need to

- a) deactivate LOOP mode and
- b) activate flow control.

6.2 Bandwidth Control

Policing, or rate limiting, allows you to limit the data rates for a particular port on the Intellinet 8-Port Gigabit Web-Smart 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 or download), whereas egress traffic is traffic sent out (outgoing, outbound or upload) to another network client.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port	Select the desired port for rate configuration. Hold down CTRL to select multiple ports at once.
Type	Select Ingress or Egress from the drop-down box.
State	Enable or Disable bandwidth control for the selected port. Set this to enable, or the values will not be saved.
Rate	Select the maximum transmission rate for the selected ports.

Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 1	1000	Unlimited
Port 2	1000	Unlimited
Port 3	1000	Unlimited
Port 4	1000	Unlimited
Port 5	1000	Unlimited
Port 6	1000	Unlimited
Port 7	Unlimited	Unlimited
Port 8	Unlimited	Unlimited



Note:

When egress bandwidth control is enabled for one or multiple ports, it is recommended to disable flow control on each port to ensure that the switch continues to work normally.

7 Security

7.1 Storm Filter

The Storm Filter function enables the Intellinet switch to filter broadcast, multicast, unknown unicast and multicast frames in your network. If the transmission rate of these kinds of packets exceeds the set bandwidth, the packets will be automatically discarded to avoid network broadcast storm.

Select the Storm Type from the drop-down list.

Hold “Ctrl” and the left button of the mouse to select the ports you need, select Enable from the State drop-down box to enable the setting, and then choose the rate from the checkbox.

Click Apply, then the Storm Filter information will be displayed as below.

Storm Type	Port	State	Rate (kbps)
Broadcast	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Enable	256M bps

Apply

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Storm Type	Broadcast: Broadcast packets Multicast: Multicast packets Unknown Unicast: Unknown unicast packets Unknown Multicast: Unknown multicast packets
Port	Select the desired port for Storm Filter configuration. Hold down CTRL to select multiple ports at once.
State	Disable: Disable the Storm Filter function. Enable: Enable the Storm Filter function. Set this to enable, or the values will not be saved.
Rate	Select the bandwidth threshold for the specified packet type on the port. Any traffic exceeding this bandwidth rate will be discarded.

7.2 Loop Prevention

The Intellinet 8-Port Gigabit Web-Smart Switch can detect loops in your network. The loop detection feature is designed to detect loopbacks and activate the Loop LED on the front panel of the switch. Loop detection also indicates the port(s) causing the loop on the web administrator UI.

The loop prevention feature, on the other hand, blocks any port that has been deemed to be causing a loop automatically.

Loop Prevention

loop prevention setting
Loop Prevention

Note: Loop Prevention/Loop Detection can be supported only if trunk group setting is disabled.

Apply

Port	Loop State	Loop Status
Port 1	Enabled	FORWARDING
Port 2	Enabled	FORWARDING
Port 3	Enabled	FORWARDING
Port 4	Enabled	FORWARDING
Port 5	Enabled	FORWARDING
Port 6	Enabled	FORWARDING
Port 7	Enabled	FORWARDING
Port 8	Enabled	FORWARDING

Select the type of loop detection/prevention mechanism from the drop-down list, then click 'Apply.'

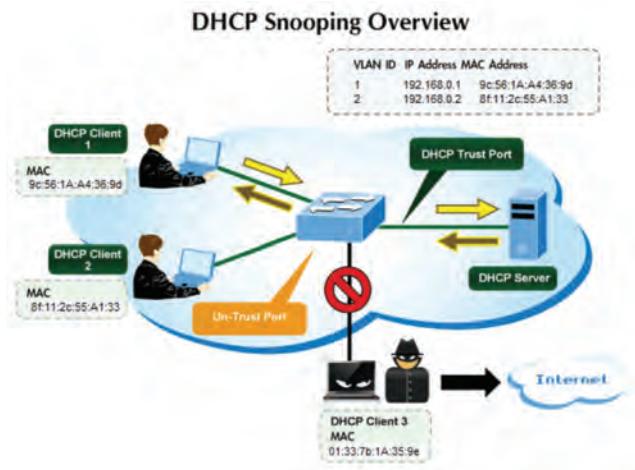


Note:

Loop prevention / detection can only be used if no trunk groups are activated.

7.3 DHCP Snooping

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP Snooping allows the Intellinet switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.



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

DHCP Snooping

DHCP Snooping Setting	Enable ▼
DHCP Server Port	Port 1 ▼
Apply	

Note: The trunk port can not be set as the DHCP server port.

Activating DHCP Snooping on the Intellinet 8-Port Gigabit Web-Smart Switch is simple: Set DHCP Snooping to 'Enable', specify the port to which the DHCP server (i.e., the router) is connected to, and then click 'Apply' to activate the settings.

8 Appendix A: Changing the IP Address of a Network Adapter

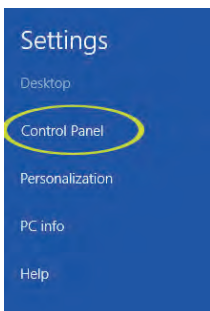
The Intellinet 8-Port Gigabit Web-Smart Switch operates on the IP address 192.168.2.1. For your computer to access the administrator configuration interface, the IP address of the network adapter in your computer has to be in the same range; e.g., 192.168.2.50. Refer to the instructions that came with your computer for information on how to change the IP address on the network adapter in your computer for any operating system that is not explained in this user manual.

8.1 Windows 8

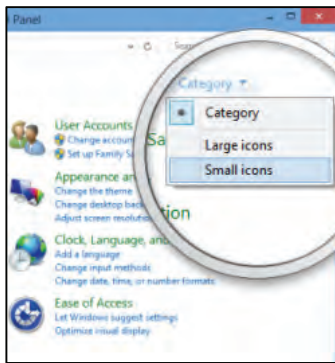
1. If you are using a PC, move the mouse cursor to the bottom or top right corner of the screen and select the cog icon for Settings. If you are using a tablet, swipe left from the right side of the screen and select Settings.



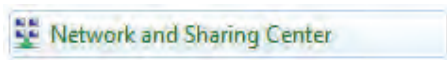
2. Click "Control Panel."



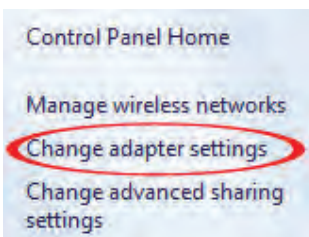
3. Select "Small icons."



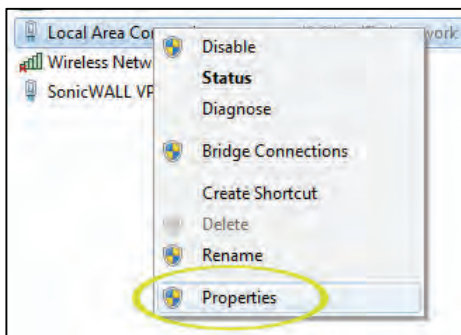
4. Open "Network and Sharing Center."



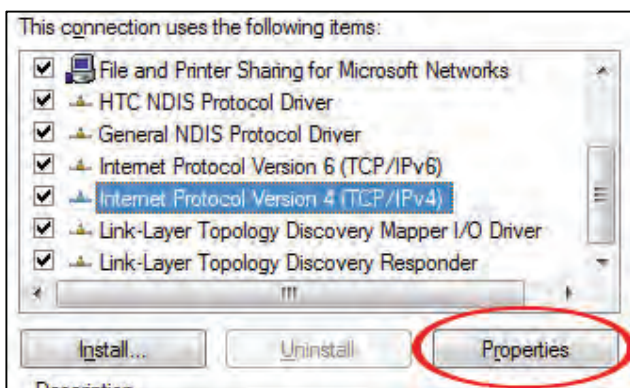
5. Click "Change adapter settings."



6. Right-click your network adapter and select "Properties."



7. Select "Internet Protocol Version 4" from the list and click "Properties."

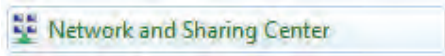


8. Enter the information as shown below, then click “OK” to save the settings.

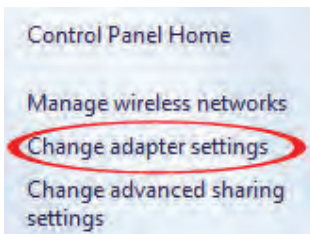
☒ Use the following IP address:	
IP address:	192 . 168 . 2 . 50
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

8.2 Windows 7 and 10

1. Open the Network and Sharing Center.

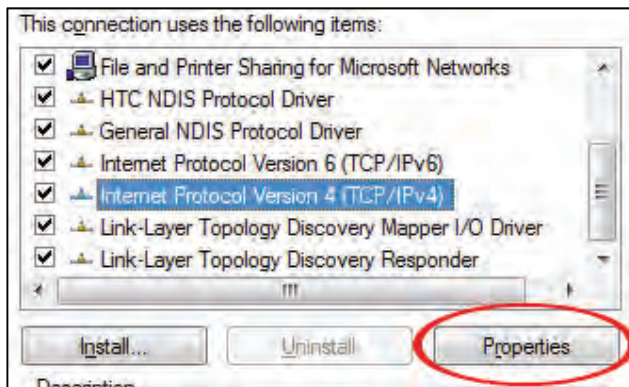


2. Click on "Change adapter settings."



3. Right-click your network adapter and select "Properties."

4. Select "Internet Protocol Version 4" from the list and click "Properties."

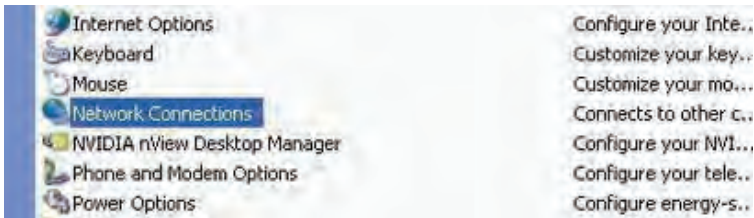


5. Enter the information as shown below, then click "OK" to save the settings.

☒ Use the following IP address:	
IP address:	192 . 168 . 2 . 50
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	.

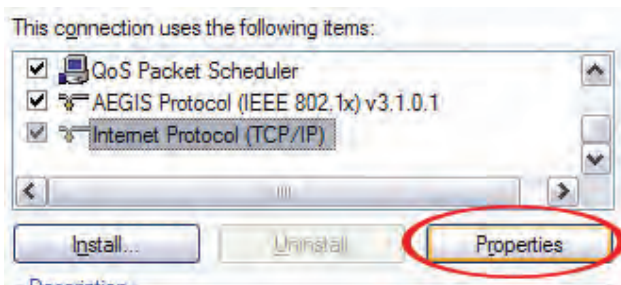
8.3 Windows XP:

1. Double-click the “Network Connections” icon in the control panel.



2. Right-click the connection (e.g., Local Area Connection) and select “Properties.”

3. Select “Internet Protocol (TCP/IP)” from the list and click “Properties.”



4. Enter the information as shown below, then click “OK” to save the settings.

☒ Use the following IP address:	
IP address:	192 . 168 . 2 . 50
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

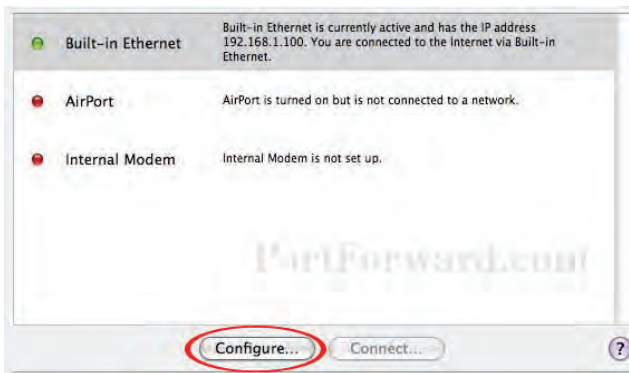
8.4 Mac OS X

1. Open the System Preferences page.

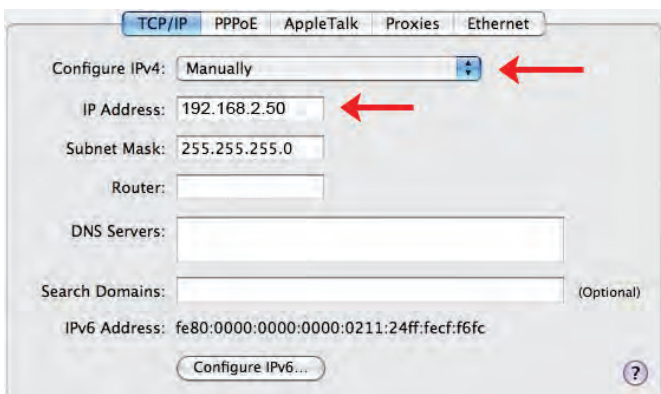
2. In the Internet & Network section, click the Network icon.



3. Select either Built-in Ethernet or AirPort, depending on how you connect to the wireless access point, then click “Configure...”



4. Set the value for Configure IPv4 to “Manually” and enter 192.168.2.50 in the IP Address field. Click “Apply Now” (not shown in screen shot) to save the settings.



9 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 fue adquirido o en el domicilio de IC Intracom México, S.A.P.I. de C.V., junto con los accesorios contenidos en 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, número de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese utilizado 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.

10 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.

11 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



Intellinetnetwork.com

© IC Intracom. All rights reserved.

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