Gigabit Ethernet PoE+ Web-Managed AV Switch

User Manual

Models 561433, 561440, 561457

Model shown: 561433

INTELLINET®
NETWORK SOLUTIONS

intellinetsolutions.com

TABLE OF CONTENTS

INTRODUCTION

Thank you for purchasing the Intellinet Network Solutions Gigabit Ethernet PoE+ Web-Managed AV Switch. Before you install and use this product, read this manual carefully for a full understanding of its functions. Because this manual applies to multiple models, the screenshots and tables may vary slightly from the actual images that your particular model offers.

PRODUCT OVERVIEW

This switch provides seamless network connections. It integrates 1000 Mbps Gigabit Ethernet, 100 Mbps Fast Ethernet and 10 Mbps Ethernet network capabilities into a highly flexible package. The switch's rear-facing ports make for a cleaner installation in the rack, so it's perfect for use in A/V environments. Each of the 10/100/1000 Mbps Auto-Negotiation RJ45 ports support Auto MDI/MDIX function.

The switch offers 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 offers a remote Web interface. You can program the switch for advanced management functions such as Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control, MAC Address Table, Diagnostics, RMON and Maintenance. Its PoE ports can automatically detect and supply power to IEEE802.3at-compliant Powered Devices (PD) such as Wireless Access Points, network cameras or Voice over IP phones.

FEATURES

- Rear-facing IEEE 802.3at/af-compliant RJ45 PoE/PoE+ Gigabit Ethernet ports
- Provides power and data connection for 8, 16 or 24 PoE network devices, depending on model
- 10/100/1000 auto-sensing ports automatically detect optimal network speeds
- Two small form-factor pluggable 1 GbE SFP module slots
- Two RJ45 combo uplink ports (model 561457)
- Console port for configuring
- Power output up to 30 watts per port*
- PoE power budget of 255 watts for models 561433 & 561440 and 425 watts for model 561457
- Supports IEEE 802.3at and IEEE 802.3af-compliant PoE devices (e.g., wireless access points, VoIP phones, IP cameras, etc.)
- Supports IEEE 802.3at/af detection and short circuit, overload and high-voltage protection
- Management by Web/SNMP/Telnet/Console
- All RJ45 ports with Auto-MDIX and NWay auto-negotiation support
- Complies with the IEEE 802.3az (Energy Efficient Ethernet [EEE]) specification
- Offers 20 Gbps switch fabric in model 561433 and 36 Gbps switch fabric in models 561440 & 561457
- SNMP Management and Remote Monitoring (RMON)
- Remote reboot/restart
- IPv4/v6 dual protocol
- Supports VLAN (tag-based and port-based)
- Provides IEEE 802.1x port-based security
- Supports link aggregation (trunking)

- Supports bandwidth control per port
- Supports port mirroring
- Supports two types of QoS: port-based and DSCP
- Broadcast storm control with multicast packet rate settings
- Support Spanning Tree Protocol IEEE 802.1d
- Store and forward switching architecture
- IEEE802.3x Flow Control
- Supports jumbo frames up to 10 kBytes
- Supports 8k MAC address entries
- LEDs for power, link/activity and PoE
- Included 19” rackmount brackets
- Included console cable

SPECIFICATIONS

STANDARDS

- IEEE 802.1d (Spanning Tree Protocol [STP])
- IEEE 802.1p (Traffic Prioritization)
- IEEE 802.1q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Tree Protocol [MSTP])
- IEEE 802.1w (Rapid Spanning Tree Protocol [RSTP])
- 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 802.3af (Power over Ethernet 802.3at Type 1)
- IEEE 802.3at (Power over Ethernet 802.3at Type 2)
- IEEE 802.3u (100Base-TX Fast Ethernet)
- IEEE 802.3x (Flow Control for full duplex mode)

POWER

- Input: 100 – 240 VAC, 50 – 60 Hz
- Power consumption: 270 W (models 561433 & 56140), 450 watts (model 561457)

ENVIRONMENTAL

- Metal housing
- Operating temperature: 0 – 40°C (32 – 104°F)
- Operating humidity: 20 – 85% RH, non-condensing
- Storage temperature: -10 – 70°C (14 – 158°F)

EXTERNAL COMPONENT DESCRIPTION

FRONT PANEL

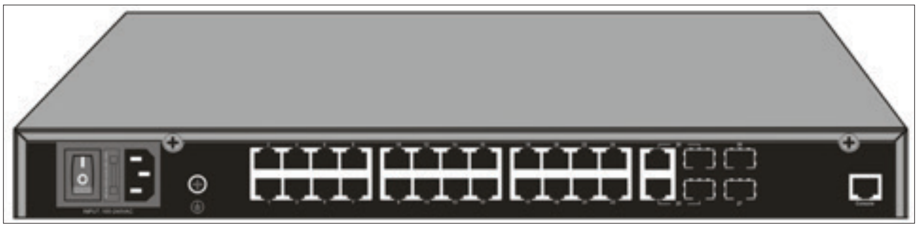
The front panel consists of LEDs that indicate status and connection:
PWR LED: Switch is connected to a power source.
Link/Act LED: Flashes indicate a network link through the corresponding port at the rear of the switch. Blinking indicates that the port is either sending or receiving data.
PoE LEDs:

- Green: a PoE powered device (PD) is connected and the port is successfully supplying power
- Off: no powered device (PD) is connected

Note: The SFP ports are shared with gigabit RJ45 ports. When an SFP port is used, the RJ45 port cannot be used.
Warning: The SFP ports should use a UL-listed Optical Transceiver product, Rated Laser Class I. 3.3 VDC (see Intellinet Solutions parts 545006, 545013, 506724, 545044, 523882).

REAR PANEL

The rear panel of the switch consists of 10/100/1000 Mbps RJ45 ports, SFP ports, one Console port, one Reset button and a series of LED indicators as shown below.



10/100/1000 Mbps RJ45 ports
Designed to connect to the device with a bandwidth of 10 Mbps, 100 Mbps or 1000 Mbps; each has a corresponding 10/100/1000 Mbps LED found at the front of the switch.
Combo ports
For installating SFP modules; offers SFP receiver slots, which are shared with the related RJ45 ports.
Console port (Console)
Connects to the serial port of a computer or terminal to monitor and configure the switch.
Power
Used to connect the included AC power cord; it supports AC 100 – 240 V, 50/60 Hz.
Switch
Turns power to the switch on or off
Fuse
Prevents power overloads and short circuits to the equipment (tank containing a spare fuse)
Grounding Terminal
Grounds the switch through the PE cable on the AC cord or with a separate ground wire.

PACKAGE CONTENTS

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

- Gigabit Ethernet PoE+ Web-Managed AV Switch
- AC power cord
- Rubber feet (4)
- Console cable
- Mounting brackets
- User Manual

INSTALLING AND CONNECTING THE SWITCH

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.

DESKTOP INSTALLATION

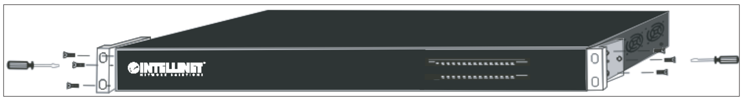
Attach the enclosed rubber feet to the bottom corners of the switch to minimize vibration. Allow adequate space for ventilation between the device and the objects around it.

INTELLINET

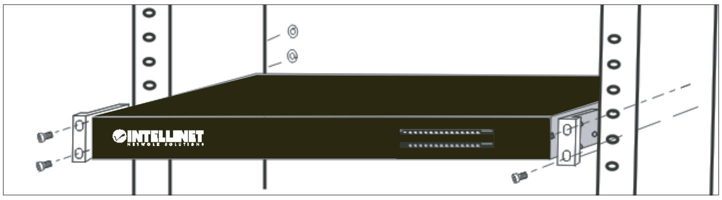
Desktop Installation

RACKMOUNT INSTALLATION IN 19" CABINET

You can mount the switch in an EIA standard-sized, 19-inch rack. To do so, attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.



Then, use the screws provided with the equipment rack to mount the switch on the rack and tighten it.



POWER ON THE SWITCH

Connecting the switch to an outlet using the AC 100-240 V, 50/60 Hz internal high-performance power supply.

AC Electrical Outlet

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.

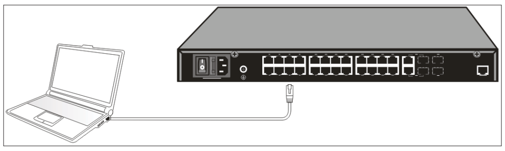
AC Power Cord Connection

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

CONNECTION TO THE SWITCH

CONNECTING TO A COMPUTER

Use standard network cable 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 they are connected to. The LNK/ACT/Speed LEDs for each port are illuminated when the link is available.



HOW TO LOG IN TO THE SWITCH

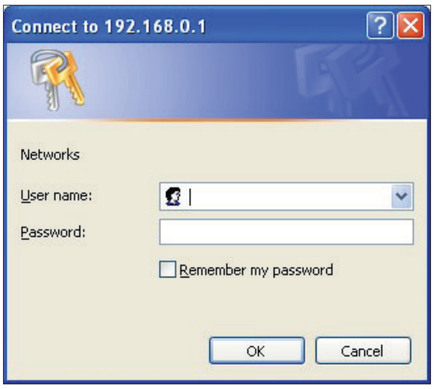
This switch provides Web-based management, This section describes how to configure the switch. The default settings of the switch are shown below.

Parameter	Default Value
Default IP address	192.168.0.1
Default Username	admin
Default Password	Switch serial number — find in label on switch underside

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: 192.168.0.xxx (“xxx” range is 2-254); for example, 192.168.0.100.

Open the browser, and go to the URL http://192.168.0.1 to access the switch login window, as shown below.



Connect to 192.168.0.1

Networks

User name: |

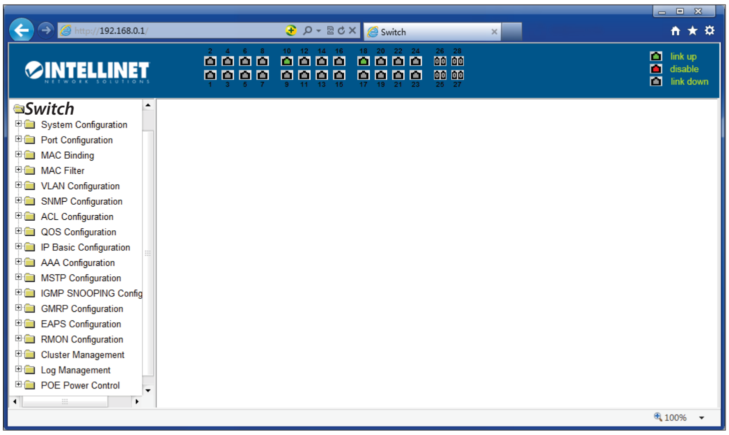
Password:

□ Remember my password

WEB PAGE ELEMENTS

INTERFACE STRUCTURE

The switch's GUI, as shown on the following pages, is composed of three parts: a header featuring the Port Status panel, a left-side Navigation Tree panel with folders and pages, and a larger-area Focus Page that shows the contents of the page you've selected from the panel. Find the page you want to manage using the Navigation Tree.



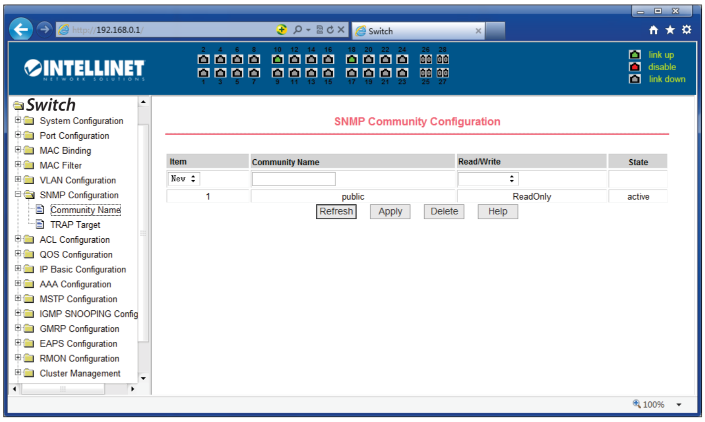
COMMON FUNCTIONS

Each page features some commonly used buttons. The function of each is described below:

Button	Effect
Refresh	Updates all fields on the page
Apply	Updates into the memory what is entereded into the editable fields. Because the Web server checks for errors, no error-checking occurs before the user selects this button.
Delete	Deletes the current record
Help	Opens online help pages

ENTRY FIELDS

To add a new line, select "New" from the drop-down menu, enter new information, and then click Apply. To edit an existing line, select the appropriate line number of the drop-down menu first, make your edits, and then click Apply. The change is then recorded and displayed in the table. To delete a row, select the line number from the entry field's drop-down menu, then press the delete key. The line will disappear from the table.

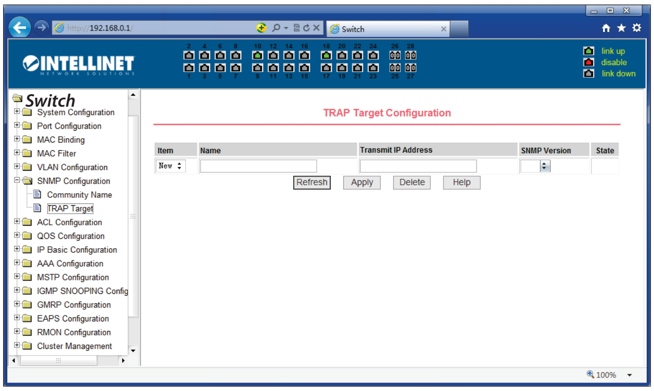


SNMP Community Configuration

Item	Community Name	Read/Write	State
New			
1	public	ReadOnly	active

STATUS FIELD

A State field will display on the far-right of some Focus Pages, which gives the status of the line displayed. All displayed status fields are Read-Only. Once information has been entered, click Apply, and the line will reflect the status.



TRAP Target Configuration

Item	Name	Transmit IP Address	SNMP Version	State
New				

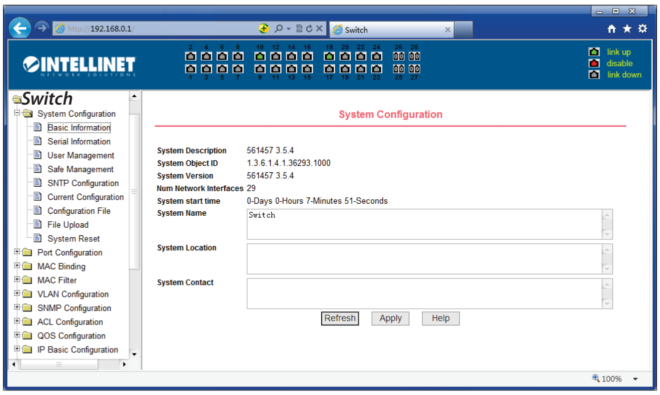
SWITCH CONFIGURATION

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

SYSTEM CONFIGURATION

BASIC INFORMATION

The following image shows basic system information, which lets you to configure the System Name, Location and Contact. Click apply to save any changes.

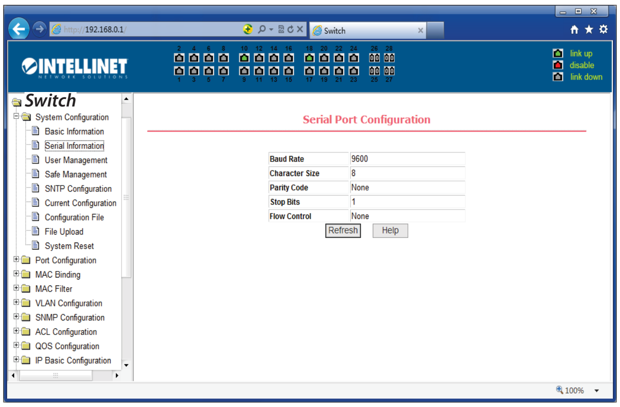


System Configuration

System Description 561457 3.5.4
System Object ID 1.3.6.1.4.1.36293.1000
System Version 561457 3.5.4
Num Network Interfaces 29
System start time 0-Days 0-Hours 7-Minutes 51-Seconds
System Name Switch
System Location
System Contact

SERIAL (CONSOLE PORT) INFORMATION

The following image shows the settings of the console port, which include Baud Rate, Character Size, Parity Code, Stop Bits, and Flow Control. Make sure settings are the same in the software on your PC.

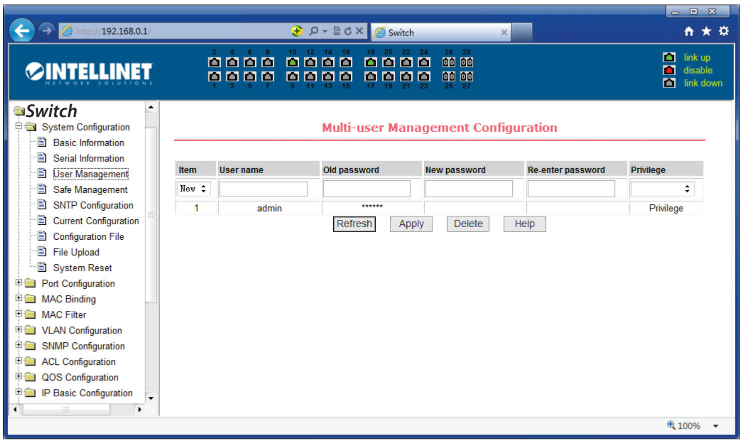


Serial Port Configuration

Baud Rate	9600
Character Size	8
Parity Code	None
Stop Bits	1
Flow Control	None

USER MANAGEMENT

The following image shows the User Management page, where you can add multiple switch users, set user names and passwords, change the admin and other passwords, and manage users.



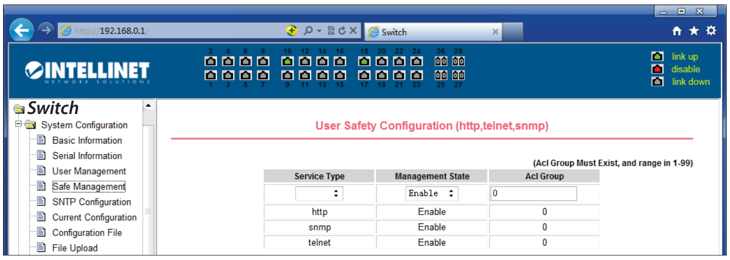
Multi-user Management Configuration

Item	User name	Old password	New password	Re-enter password	Privilege
New					
1	admin	******			Privilege

Refresh Apply Delete Help

SAFE MANAGEMENT

The following image shows how to connect to the interface of the switch through the web GUI, TELNET and SNMP functions. An administrator can control network management services such as TELNET, WEB and SNMP as well as enable (default) or disable these services. ACL groups can also be assigned here. More information on this is available under ACL configuration later in the manual.



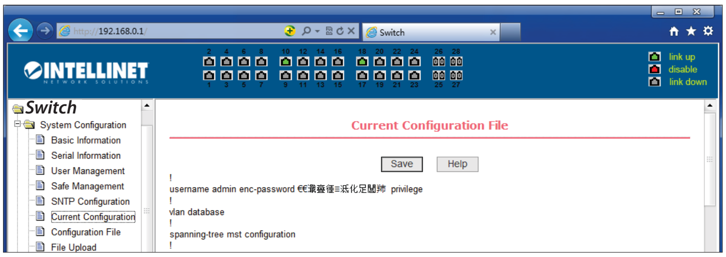
User Safety Configuration (http,telnet,snmp)

(Acl Group Must Exist, and range in 1-99)

Service Type	Management State	Acl Group
	Enable	0
http	Enable	0
snmp	Enable	0
telnet	Enable	0

CURRENT CONFIGURATION

This page shows the current configuration. Also known as "Running Config," this screen lets the user view the current configuration of the switch. Clicking Save files the current configuration in the Configuration File option in the left menu.

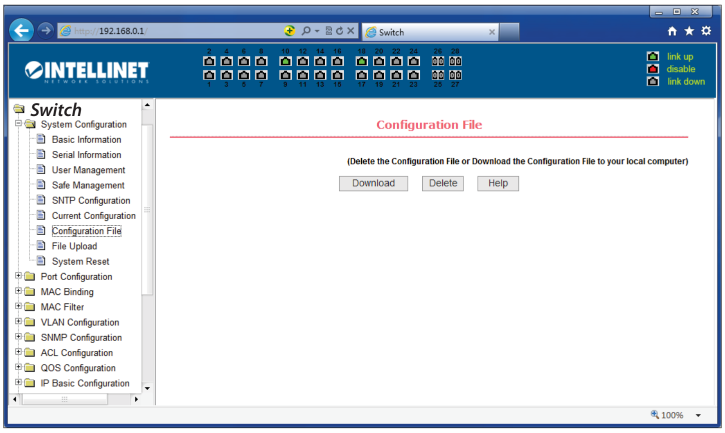


Current Configuration File

```
!
username admin enc-password €€澉蝵徸=泜化足閶鈽  privilege
!
vlan database
!
spanning-tree mst configuration
!
```

CONFIGURATION FILE

This the current “Running Configuration” of the switch created from the previous menu option.

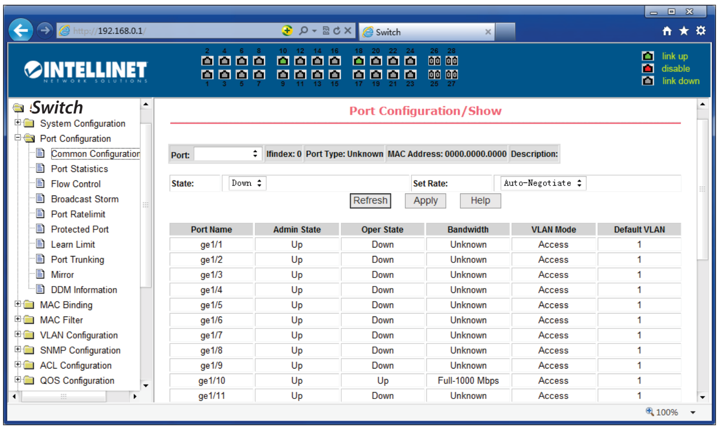


Configuration File

(Delete the Configuration File or Download the Configuration File to your local computer)

PORT CONFIGURATION/SHOW

The following image shows the Port Configuration/Show page. Through this page, users can enable or disable ports, set the port speed or view the basic information of all ports.



Port Configuration/Show

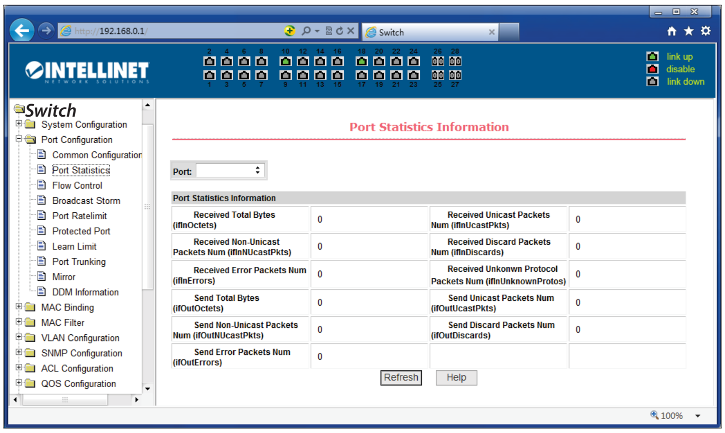
Port: Ifindex: 0 Port Type: Unknown MAC Address: 0000.0000.0000 Description:

State: Down Set Rate: Auto-Negotiate

Port Name	Admin State	Oper State	Bandwidth	VLAN Mode	Default VLAN
ge1/1	Up	Down	Unknown	Access	1
ge1/2	Up	Down	Unknown	Access	1
ge1/3	Up	Down	Unknown	Access	1
ge1/4	Up	Down	Unknown	Access	1
ge1/5	Up	Down	Unknown	Access	1
ge1/6	Up	Down	Unknown	Access	1
ge1/7	Up	Down	Unknown	Access	1
ge1/8	Up	Down	Unknown	Access	1
ge1/9	Up	Down	Unknown	Access	1
ge1/10	Up	Up	Full-1000 Mbps	Access	1
ge1/11	Up	Down	Unknown	Access	1

PORT STATISTICS

The following image shows the port statistics information page. To view a particular port, select the appropriate port name in the port drop-down menu. This page also allows you to view the statistics of all packets.



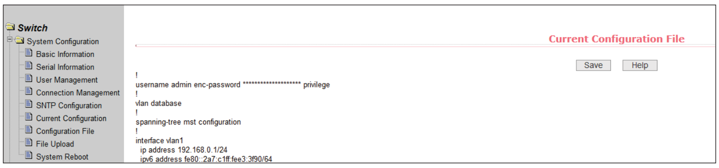
Port Statistics Information

Port:

Port Statistics Information			
Received Total Bytes (ifInOctets)	0	Received Unicast Packets Num (ifInUcastPkts)	0
Received Non-Unicast Packets Num (ifInNUcastPkts)	0	Received Discard Packets Num (ifInDiscards)	0
Received Error Packets Num (ifInErrors)	0	Received Unkonwn Protocol Packets Num (ifInUnknownProtos)	0
Send Total Bytes (ifOutOctets)	0	Send Unicast Packets Num (ifOutUcastPkts)	0
Send Non-Unicast Packets Num (ifOutNUcastPkts)	0	Send Discard Packets Num (ifOutDiscards)	0
Send Error Packets Num (ifOutErrors)	0		

FLOW CONTROL

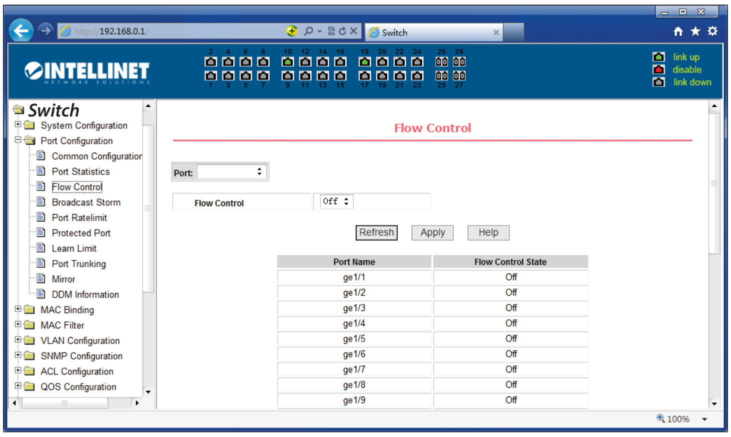
IEEE 802.3x Flow Control is the process of managing the rate of data transmission between two nodes (i.e., the switch and a connected network client) to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving 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.



Current Configuration File

```
!
username admin enc-password ******************** privilege
!
vlan database
!
spanning-tree mst configuration
!
interface vlan1
  ip address 192.168.0.1/24
  ipv6 address fe80::2a7:c1ff:fee3:3f90/64
```

The following image shows the options for Flow Control. Users can enable and disable the Flow Control of each port here.



Flow Control

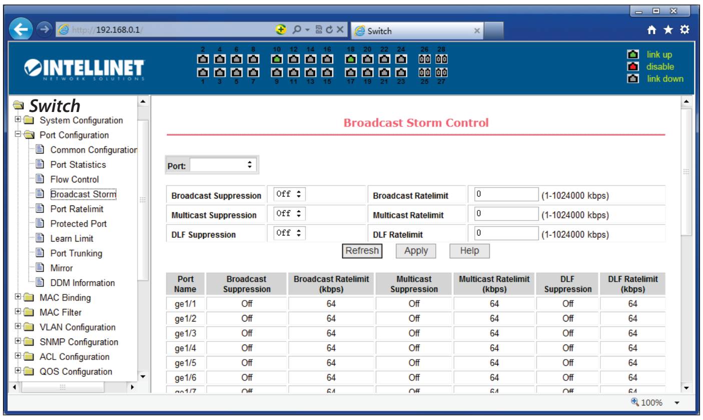
Port:

Flow Control: Off

Port Name	Flow Control State
ge1/1	Off
ge1/2	Off
ge1/3	Off
ge1/4	Off
ge1/5	Off
ge1/6	Off
ge1/7	Off
ge1/8	Off
ge1/9	Off

BROADCAST STORM CONTROL

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 switch allows configuring maximum allowed pps rates for three different types of packets (Broadcast, Multicast and Unicast). The following image shows the Broadcast Storm Control page. This page is used to turn on or off Broadcast, Multicast and DLF Suppressions and apply a rate limit. The default rate limit is 64 kbps.



Broadcast Storm Control

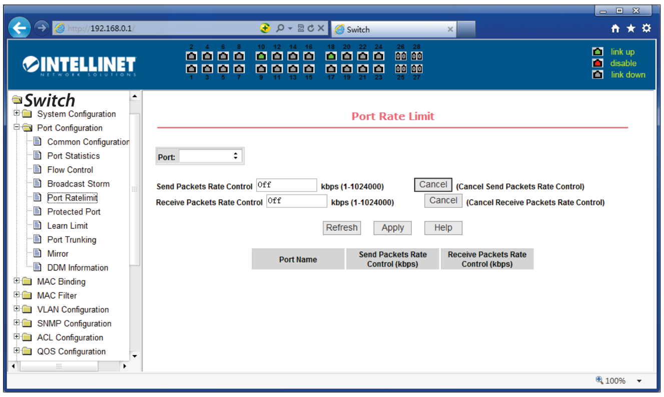
Port:

Broadcast Suppression	Off	Broadcast Ratelimit	0 (1-1024000 kbps)
Multicast Suppression	Off	Multicast Ratelimit	0 (1-1024000 kbps)
DLF Suppression	Off	DLF Ratelimit	0 (1-1024000 kbps)

Port Name	Broadcast Suppression	Broadcast Ratelimit (kbps)	Multicast Suppression	Multicast Ratelimit (kbps)	DLF Suppression	DLF Ratelimit (kbps)
ge1/1	Off	64	Off	64	Off	64
ge1/2	Off	64	Off	64	Off	64
ge1/3	Off	64	Off	64	Off	64
ge1/4	Off	64	Off	64	Off	64
ge1/5	Off	64	Off	64	Off	64
ge1/6	Off	64	Off	64	Off	64
ge1/7	Off	64	Off	64	Off	64

PORT SPEED LIMITS

This feature allows you to limit the data rates for a particular port on the Switch. When the data rate exceeds user-configured values, the 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 following image shows the Port Speed-Limit page. This page is used to configure the send and receive rate of the port.



Port Rate Limit

Port:

Send Packets Rate Control Off kbps (1-1024000) Cancel (Cancel Send Packets Rate Control)

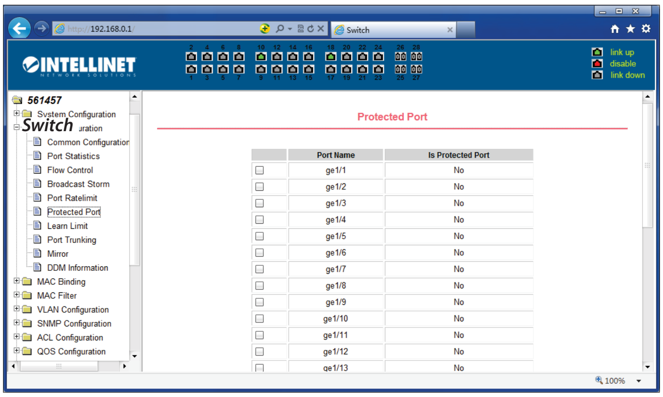
Receive Packets Rate Control Off kbps (1-1024000) Cancel (Cancel Receive Packets Rate Control)

Refresh Apply Help

Port Name	Send Packets Rate Control (kbps)	Receive Packets Rate Control (kbps)

PORT ISOLATION

The following image shows the page for Port Protection. Port isolation prevents network clients, such as PCs on different ports, from communicating with each other without the necessity of configuring a VLAN.

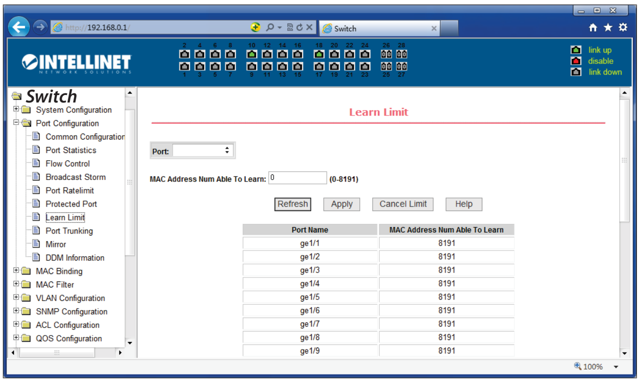


Protected Port

	Port Name	Is Protected Port
□	ge1/1	No
□	ge1/2	No
□	ge1/3	No
□	ge1/4	No
□	ge1/5	No
□	ge1/6	No
□	ge1/7	No
□	ge1/8	No
□	ge1/9	No
□	ge1/10	No
□	ge1/11	No
□	ge1/12	No
□	ge1/13	No

PORT LEARNING LIMIT

The following image shows the Learn Limit of the each port. This page is used to restrict how many MAC addresses the port is allowed to learn. The default value is the maximum of 8191.



Learn Limit

Port:

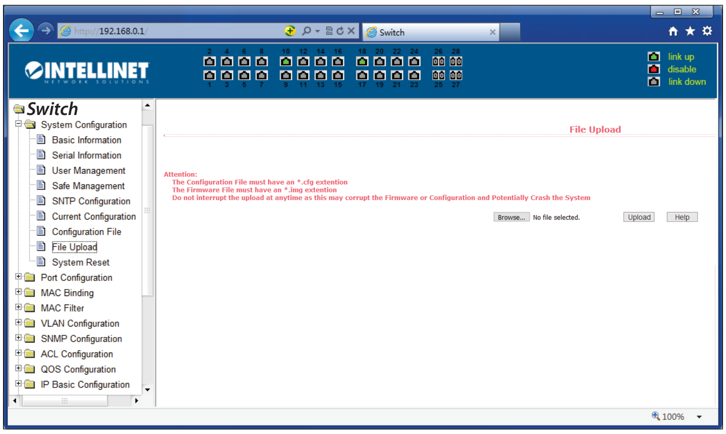
MAC Address Num Able To Learn: 0 (0-8191)

Refresh Apply Cancel Limit Help

Port Name	MAC Address Num Able To Learn
ge1/1	8191
ge1/2	8191
ge1/3	8191
ge1/4	8191
ge1/5	8191
ge1/6	8191
ge1/7	8191
ge1/8	8191
ge1/9	8191

FILE UPLOAD

The following image shows that you can restore the settings from the configuration in the previous menu option and upload it here.



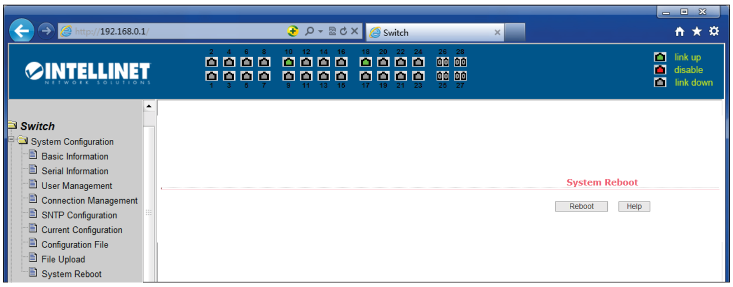
File Upload

Attention:
The Configuration File must have an *.cfg extention
The Firmware File must have an *.img extention
Do not interrupt the upload at anytime as this may corrupt the Firmware or Configuration and Potentially Crash the System

No file selected.

SYSTEM REBOOT

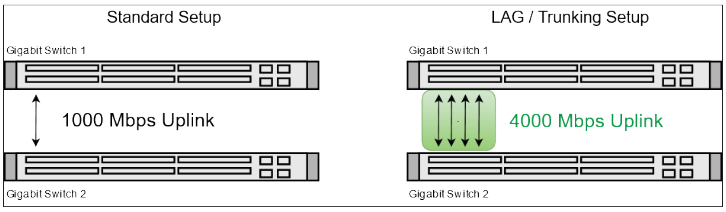
The following image shows that you can reboot the switch from this section.



System Reboot

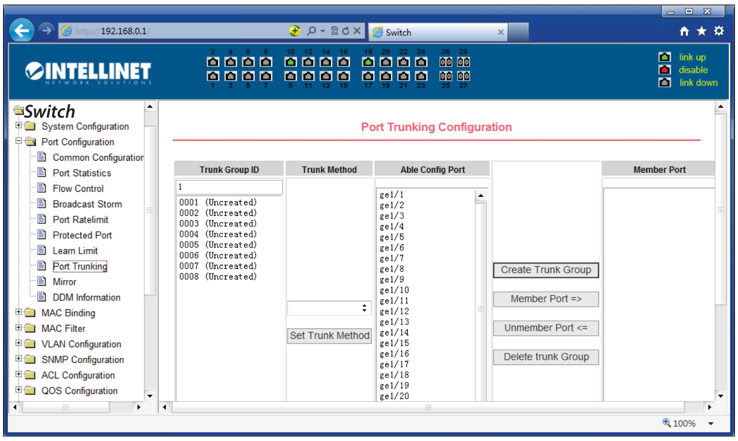
PORT TRUNKING CONFIGURATION (A.K.A. PORT AGGREGATION)

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.

The following image shows the Port-Trunking Configuration page. Here, we can create a trunk ID (eight maximum), set the trunk method, and assign a port to a group. The six trunk methods can be src-MAC, dst-MAC, src-dst-MAC, src-ip, dst-ip, src-dst-ip.



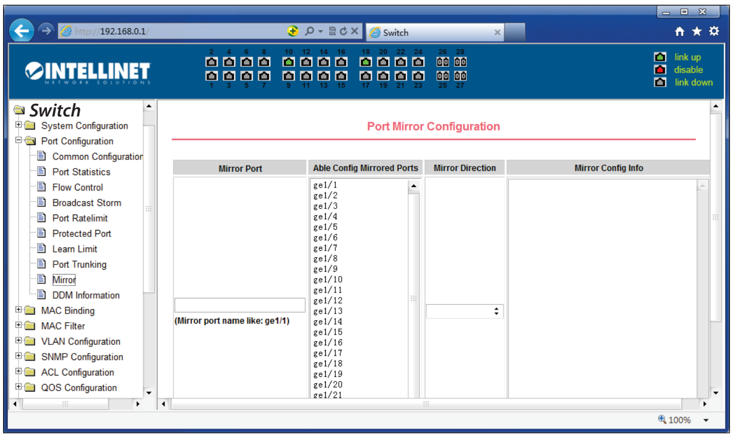
Port Trunking Configuration

Trunk Group ID	Trunk Method	Able Config Port	Member Port
1 0001 (Uncreated) 0002 (Uncreated) 0003 (Uncreated) 0004 (Uncreated) 0005 (Uncreated) 0006 (Uncreated) 0007 (Uncreated) 0008 (Uncreated)		ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20	

PORT MIRROR CONFIGURATION

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 following image shows the Port Mirroring Configuration page, which allows the activity of one port to be duplicated to another. We can choose to duplicate the data being received, transmitted, or both or not at all.



Port Mirror Configuration

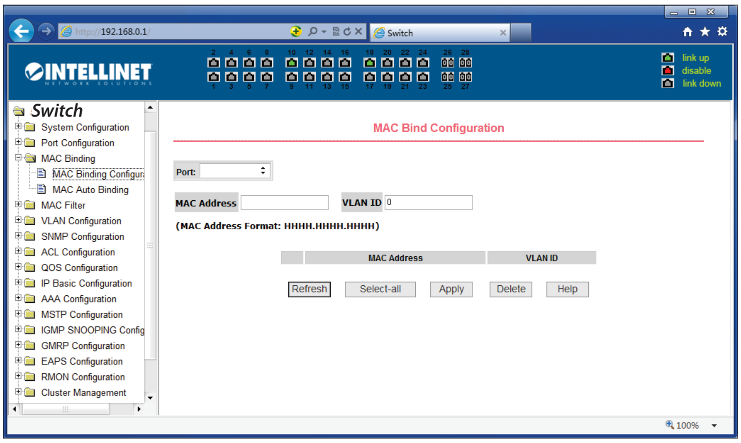
Mirror Port	Able Config Mirrored Ports	Mirror Direction	Mirror Config Info
(Mirror port name like: ge1/1)	ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21		

MAC BINDING

MAC BIND CONFIGURATION

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.

The following image shows the MAC binding configuration page, where users can manually bind a MAC address to a specified port.



MAC Bind Configuration

Port:

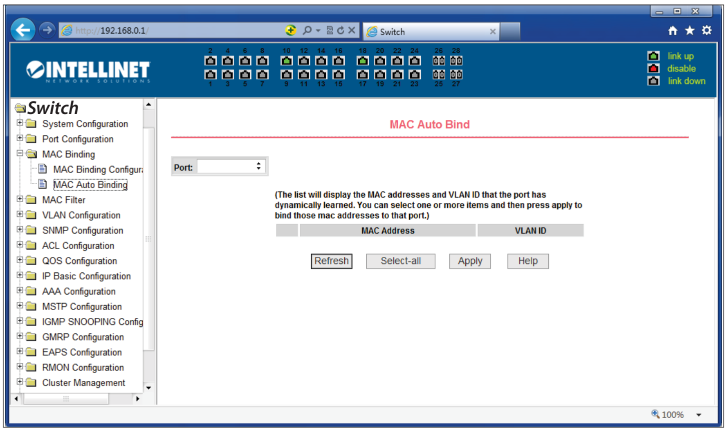
MAC Address VLAN ID 0

(MAC Address Format: HHHH.HHHH.HHHH)

	MAC Address	VLAN ID

MAC BINDING AUTOMATIC CONVERSION

The following image shows the MAC Auto Bind configuration page. This page allows users to let the switch automatically bind a MAC address to a port upon its first use.



MAC Auto Bind

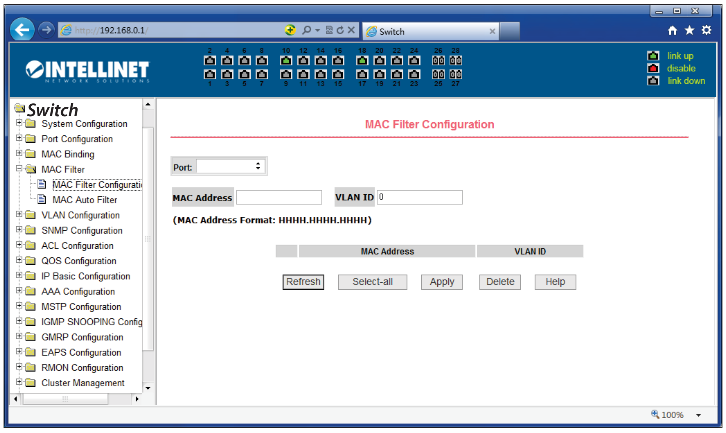
Port:

(The list will display the MAC addresses and VLAN ID that the port has dynamically learned. You can select one or more items and then press apply to bind those mac addresses to that port.)

	MAC Address	VLAN ID

MAC FILTER CONFIGURATION

The following image shows the MAC Filter Configuration page, where users can manually map a port and a MAC address together.



MAC Filter Configuration

Port:

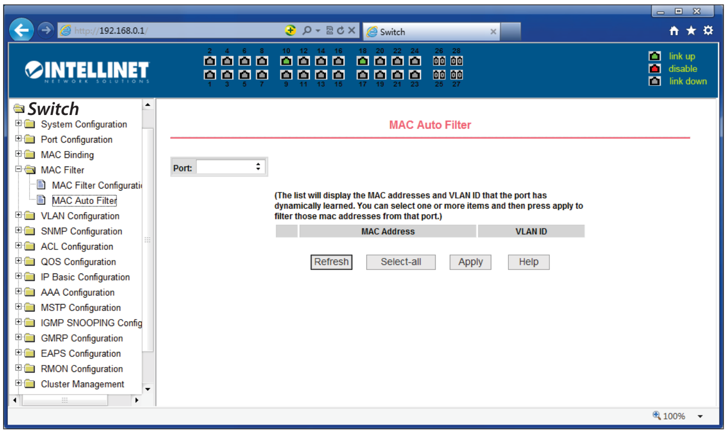
MAC Address VLAN ID 0

(MAC Address Format: HHHH.HHHH.HHHH)

	MAC Address	VLAN ID

MAC FILTERING AUTOMATIC CONVERSION

The following image shows the MAC Auto Filter page, which automatically maps the MAC addresses to the port.



MAC Auto Filter

Port:

(The list will display the MAC addresses and VLAN ID that the port has dynamically learned. You can select one or more items and then press apply to filter those mac addresses from that port.)

	MAC Address	VLAN ID

Refresh Select-all Apply Help

VLAN CONFIGURATION

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:

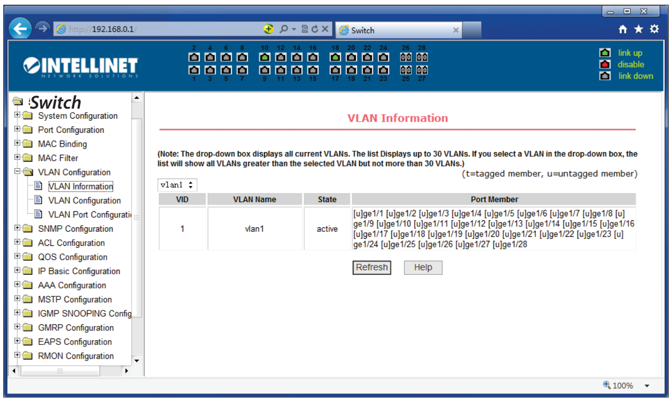
1. Broadcast traffic does not cross into different VLANs, which reduces bandwidth utilization and improves network performance.
2. Security in your LAN can be improved, since packets in different VLANs cannot communicate with each other directly.
3. With VLAN, clients can be allocated to different working groups, and users from the same group do not have to be *Switch* 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)
    1. Access ports are designed to tag any incoming packet with the VLAN ID the port has been assigned to.
    2. Tagged VLAN packets arriving at the access port are dropped by the switch.
    3. 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)
    1. 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.
    2. Trunk ports do not remove any existing VLAN tags from incoming packets.
    3. Trunk ports do not add a VLAN tag to any incoming untagged packet.
    4. 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
    1. These are a combination of access and trunk ports.
    2. Hybrid ports will tag any incoming packet that has no VLAN ID with the VLAN ID the port has been assigned to.
    3. Hybrid ports will also act as trunk ports for packets that have a VLAN tag.

VLAN INFORMATION

The following image shows the current VLAN configuration.



VLAN Information

(Note: The drop-down box displays all current VLANs. The list Displays up to 30 VLANs. If you select a VLAN in the drop-down box, the list will show all VLANs greater than the selected VLAN but not more than 30 VLANs.)

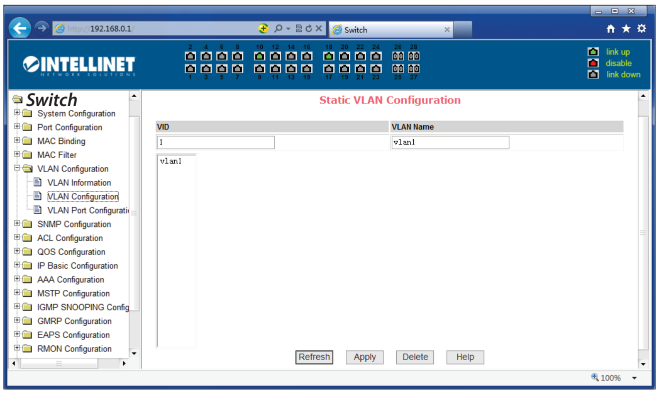
(t=tagged member, u=untagged member)

vlan1

VID	VLAN Name	State	Port Member
1	vlan1	active	[u]ge1/1 [u]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10 [u]ge1/11 [u]ge1/12 [u]ge1/13 [u]ge1/14 [u]ge1/15 [u]ge1/16 [u]ge1/17 [u]ge1/18 [u]ge1/19 [u]ge1/20 [u]ge1/21 [u]ge1/22 [u]ge1/23 [u]ge1/24 [u]ge1/25 [u]ge1/26 [u]ge1/27 [u]ge1/28

STATIC VLAN CONFIGURATION

The following image shows the Static VLAN Configuration page, which allows users to create VLANs. To create a new VLAN, manually insert the VLAN ID number into the VID field and click apply. VLAN IDs can range between 2 to 4094. To delete a VLAN, click on the appropriate entry and press delete. As the default setting, VLAN1 cannot be removed.



Static VLAN Configuration

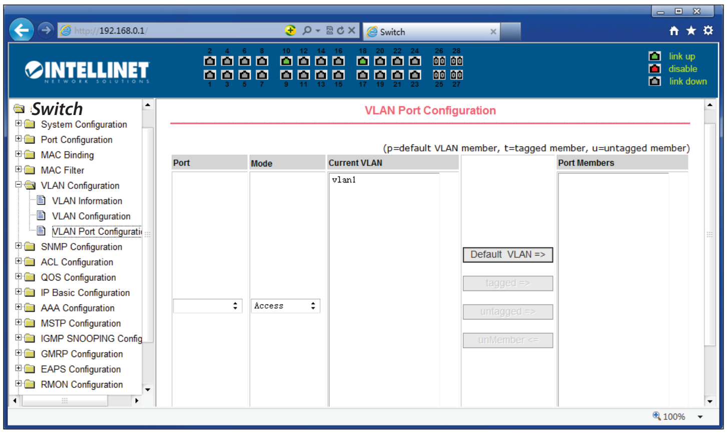
VID: 1

VLAN Name: vlan1

vlan1

VLAN PORT CONFIGURATION

The following image shows the VLAN Port Configuration page, which consists of four sections: Port, Mode, Current VLAN, and Port Members. "Port" refers to one of the ports on the switch. "Mode" refers to one of three settings: Access, Trunk and Hybrid ports (described above in more detail). "Current VLAN" refers to the current configured VLANs. "Port Members" refers to the ports assigned to the VLANs, and members listed here can be tagged, untagged or removed.



VLAN Port Configuration

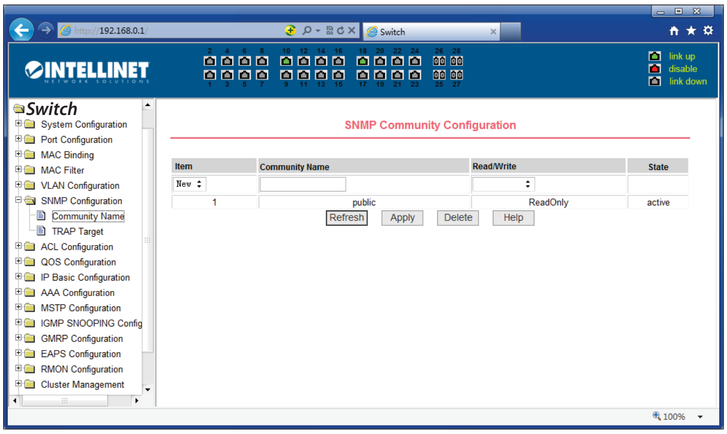
(p=default VLAN member, t=tagged member, u=untagged member)

Port | Mode: Access | Current VLAN: vlan1 | Port Members

SNMP COMMUNITY CONFIGURATION

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.

The following image shows the SNMP community configuration page, which allows users to view the configured communities and their properties or add new communities and assign properties. A total of 8 entries can be configured.

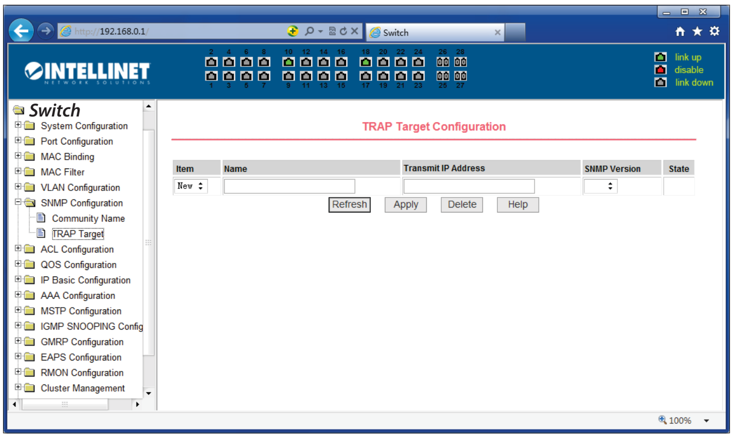


SNMP Community Configuration

Item	Community Name	Read/Write	State
New			
1	public	ReadOnly	active

TRAP TARGET CONFIGURATION

The following image shows the TRAP target configuration page, allowing users to configure workstations/ network clients that can receive TRAP messages. Users can create a custom name for the target at its IP address and the version of SNMP required.



TRAP Target Configuration

Item	Name	Transmit IP Address	SNMP Version	State
New				

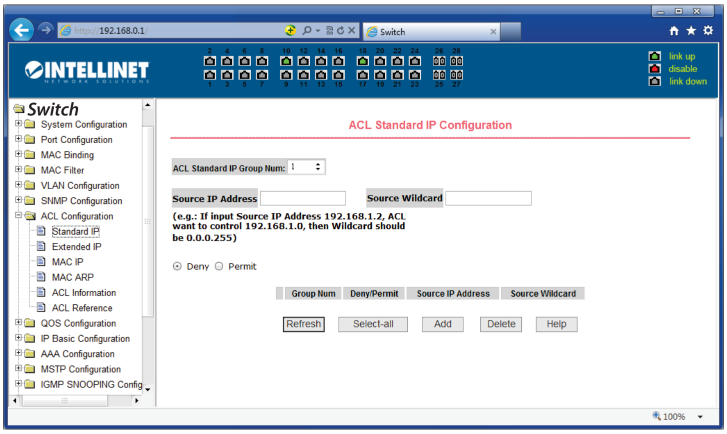
ACL CONFIGURATION

IP STANDARD ACL CONFIGURATION

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.
The following image shows the IP standard ACL configuration page, which allows users to build multiple ACL standard IP-rule bases. To create one or more rules, first select an ACL group number. Then, input IP addresses into the fields below. A rule can match only the source IP address field (with mask). The standard IP rules control the source IP address packet forwarding.



ACL Standard IP Configuration

ACL Standard IP Group Num: 1

Source IP Address Source Wildcard

(e.g.: If input Source IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255)

● Deny ○ Permit

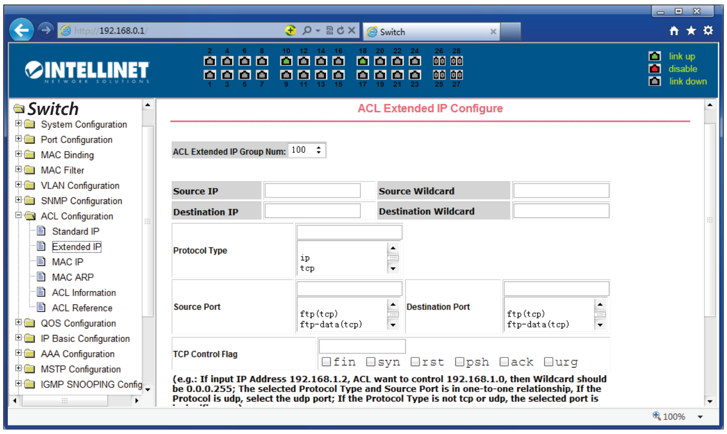
	Group Num	Deny/Permit	Source IP Address	Source Wildcard

Refresh | Select-all | Add | Delete | Help

To configure the rules, the source IP address must have a mask; the rule can match a range of IP addresses. Example:- If the rule is needed for the IP address range from 192.168.0.0 to 192.168.0.255, then the IP address would be 192.168.0.1, and its mask 0.0.0.255. Note: each rule must have a filter mode: allow or deny. The system will automatically give each rule a number. When a rule is deleted, the system will automatically resort to the existing rule sort order.

IP EXTENDED ACL CONFIGURATION

The following image shows the IP extended ACL configuration page. The extended IP group is an extension of the standard IP rules. Packet forwarding can be configured via source IP, Destination IP, IP protocol type or service port.



ACL Extended IP Configure

ACL Extended IP Group Num: 100

Source IP Source Wildcard
Destination IP Destination Wildcard

Protocol Type: ip / tcp

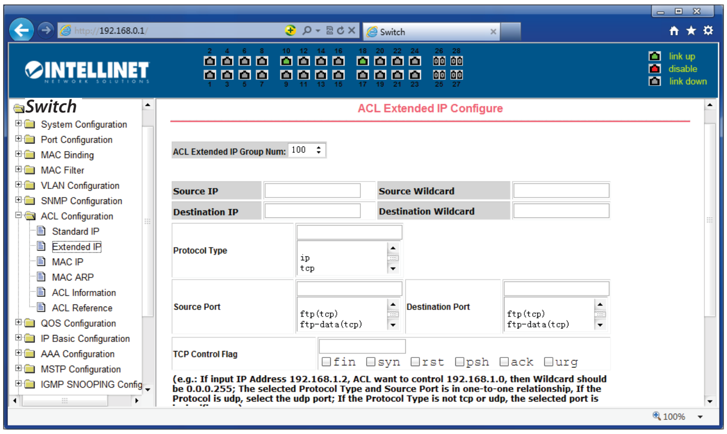
Source Port: ftp(tcp) / ftp-data(tcp) Destination Port: ftp(tcp) / ftp-data(tcp)

TCP Control Flag: □fin □syn □rst □psh □ack □urg

(e.g.: If input IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255; The selected Protocol Type and Source Port is in one-to-one relationship, If the Protocol is udp, select the udp port; If the Protocol Type is not tcp or udp, the selected port is

MAC IP ACL CONFIGURATION

The following image shows the MAC IP ACL configuration page. An IP MAC group can be configured via IP packet source and destination MAC address or source and destination IP address.



ACL Extended IP Configure

ACL Extended IP Group Num: 100

Source IP		Source Wildcard	
Destination IP		Destination Wildcard	

Protocol Type: ip, tcp

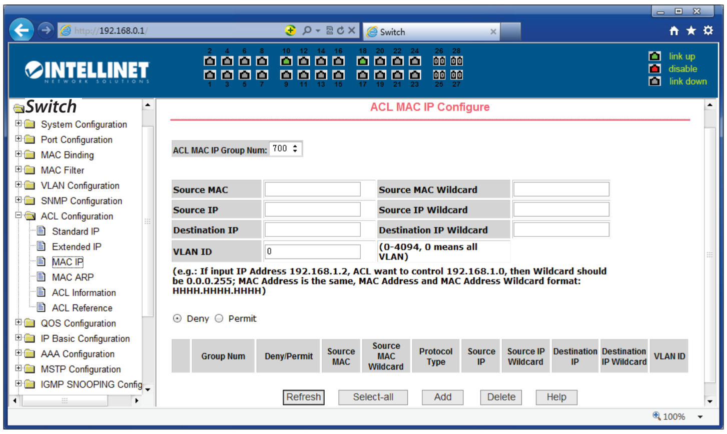
Source Port: ftp(tcp), ftp-data(tcp) Destination Port: ftp(tcp), ftp-data(tcp)

TCP Control Flag: □fin □syn □rst □psh □ack □urg

(e.g.: If input IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255; The selected Protocol Type and Source Port is in one-to-one relationship, If the Protocol is udp, select the udp port; If the Protocol Type is not tcp or udp, the selected port is

MAC IP ACL CONFIGURATION

The following image shows the MAC IP ACL configuration page. An IP MAC group can also be configured via IP packet source and destination MAC address or source and destination IP address.



ACL MAC IP Configure

ACL MAC IP Group Num: 700

Source MAC		Source MAC Wildcard	
Source IP		Source IP Wildcard	
Destination IP		Destination IP Wildcard	
VLAN ID	0	(0-4094, 0 means all VLAN)	

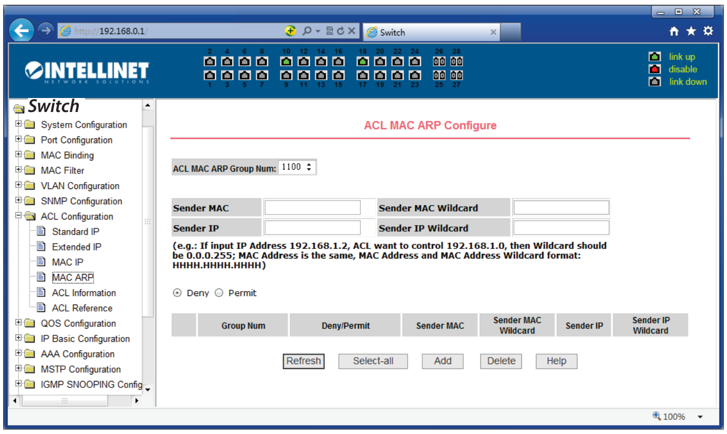
(e.g.: If input IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255; MAC Address is the same, MAC Address and MAC Address Wildcard format: HHHH.HHHH.HHHH)

● Deny ○ Permit

	Group Num	Deny/Permit	Source MAC	Source MAC Wildcard	Protocol Type	Source IP	Source IP Wildcard	Destination IP	Destination IP Wildcard	VLAN ID

MAC ARP ACL CONFIGURATION

The following image shows the MAC ARP ACL configuration page. The configuration is managed in the same way as the previous screens.



ACL MAC ARP Configure

ACL MAC ARP Group Num: 1100

Sender MAC		Sender MAC Wildcard	
Sender IP		Sender IP Wildcard	

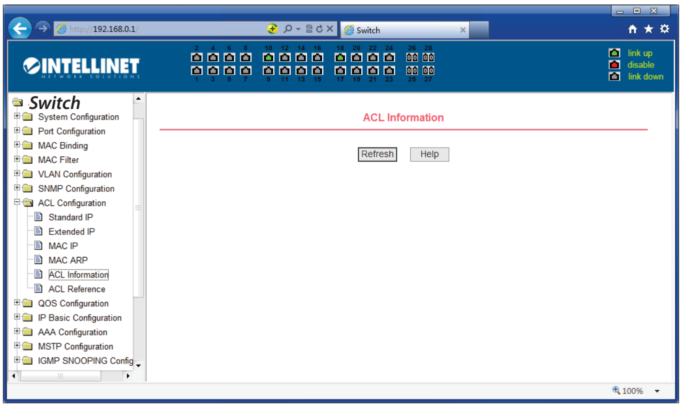
(e.g.: If input IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255; MAC Address is the same, MAC Address and MAC Address Wildcard format: HHHH.HHHH.HHHH)

● Deny ○ Permit

	Group Num	Deny/Permit	Sender MAC	Sender MAC Wildcard	Sender IP	Sender IP Wildcard

ACL INFORMATION

The following image shows the ACL information page, which displays the current ACL rules configured.



ACL Information

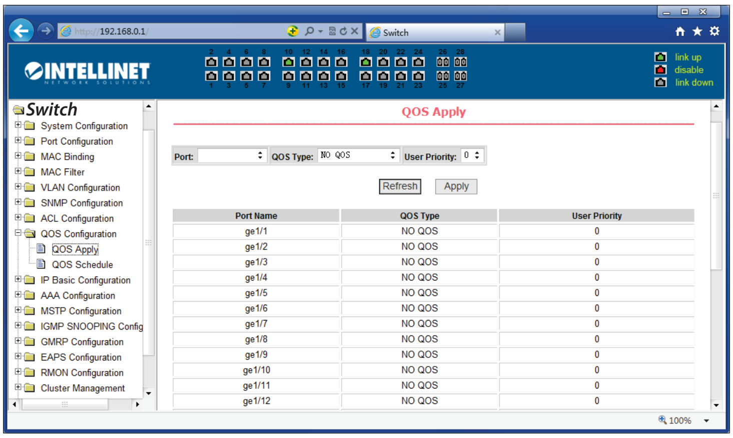
QOS CONFIGURATION

QOS APPLY CONFIGURATION

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables the assigning of 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 data and allows for the prioritization certain applications across your network. Define exactly how you want the switch to treat selected applications and types of traffic. Use QoS on your system to control a wide variety of network traffic by:

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

The following image shows a QoS Apply configuration page.



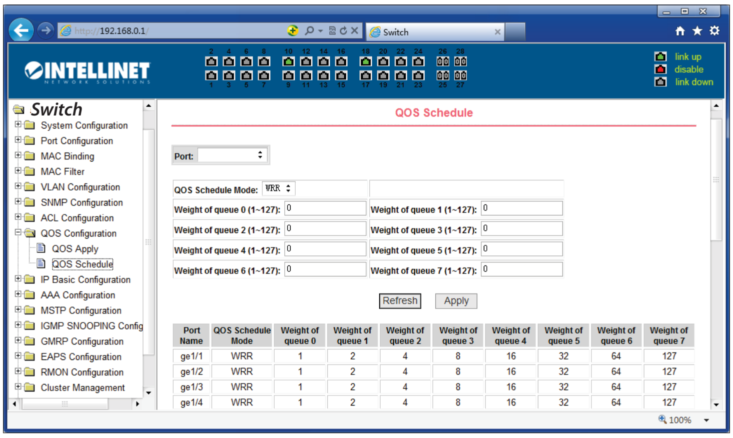
QOS Apply

Port: QOS Type: NO QOS User Priority: 0

Port Name	QOS Type	User Priority
ge1/1	NO QOS	0
ge1/2	NO QOS	0
ge1/3	NO QOS	0
ge1/4	NO QOS	0
ge1/5	NO QOS	0
ge1/6	NO QOS	0
ge1/7	NO QOS	0
ge1/8	NO QOS	0
ge1/9	NO QOS	0
ge1/10	NO QOS	0
ge1/11	NO QOS	0
ge1/12	NO QOS	0

QOS SCHEDULE CONFIGURATION

The following image shows a QoS Schedule configuration page.



QOS Schedule

Port:

QOS Schedule Mode: WRR

Weight of queue 0 (1~127): 0
Weight of queue 1 (1~127): 0
Weight of queue 2 (1~127): 0
Weight of queue 3 (1~127): 0
Weight of queue 4 (1~127): 0
Weight of queue 5 (1~127): 0
Weight of queue 6 (1~127): 0
Weight of queue 7 (1~127): 0

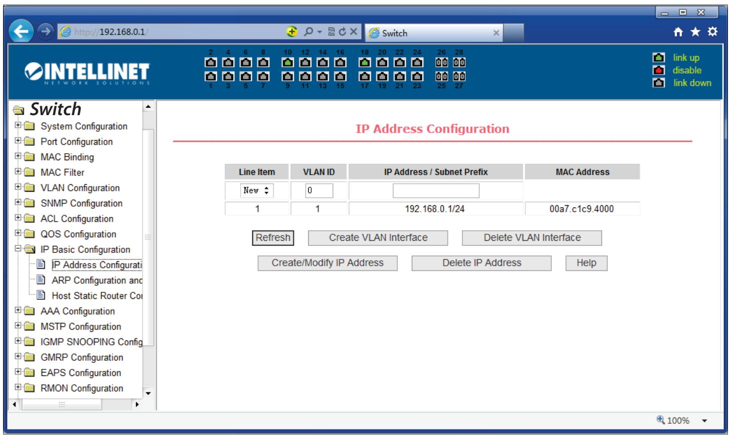
Port Name	QOS Schedule Mode	Weight of queue 0	Weight of queue 1	Weight of queue 2	Weight of queue 3	Weight of queue 4	Weight of queue 5	Weight of queue 6	Weight of queue 7
ge1/1	WRR	1	2	4	8	16	32	64	127
ge1/2	WRR	1	2	4	8	16	32	64	127
ge1/3	WRR	1	2	4	8	16	32	64	127
ge1/4	WRR	1	2	4	8	16	32	64	127

IP BASIC CONFIGURATION

IP ADDRESS CONFIGURATION FOR VLAN INTERFACES

The following image shows a VLAN interface configuration page. From this screen, it is possible to:

- Create VLAN interfaces,
- Delete VLAN interfaces,
- Configure/modify the interface IP address,
- Remove the interface IP address and view interface information.



IP Address Configuration

Line Item	VLAN ID	IP Address / Subnet Prefix	MAC Address
New	0		
1	1	192.168.0.1/24	00a7.c1c9.4000

The default configuration includes VLAN1, which cannot be deleted.

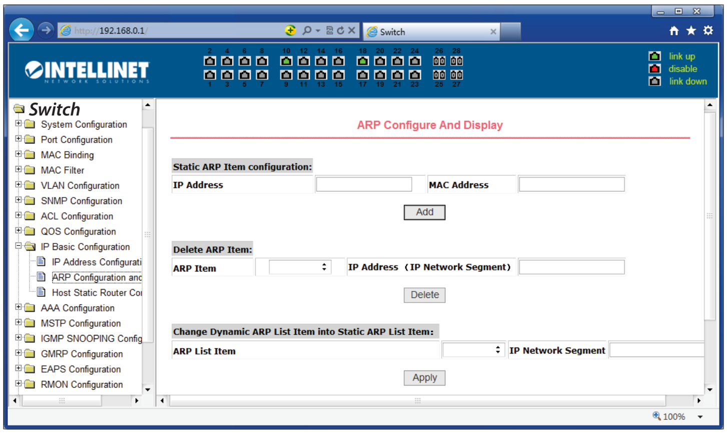
ARP CONFIGURATION AND DISPLAY

ARP is the acronym for Address Resolution Protocol. It is an internet protocol that gets the MAC address of a host or node and creates a local database or table that maps the MAC address to the host's IP address. ARP needs the IP address because the IP must have the address of a destination host before it can direct data to it.

The following image shows the ARP Configuration and Display page, from this screen it is possible to:

- Display all of the information contained in the switch ARP table.
- Configure static ARP entries,
- Delete ARP entries,
- Configure a dynamic ARP table entry as a static ARP table entry.

When a user configures a static ARP entry, the IP address and MAC address is needed (the MAC address must be a unicast MAC address).



ARP Configure And Display

Static ARP Item configuration:

IP Address | MAC Address

Delete ARP Item:

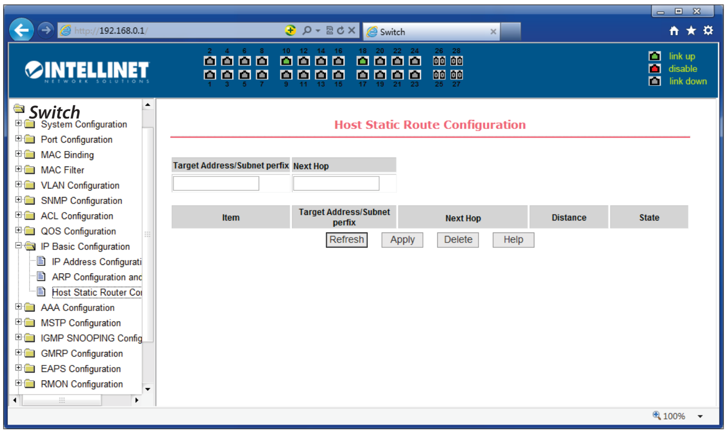
ARP Item | IP Address (IP Network Segment)

Change Dynamic ARP List Item into Static ARP List Item:

ARP List Item | IP Network Segment

HOST STATIC ROUTING CONFIGURATION

The following image shows the host static route configuration page. From this screen it is possible to add and delete static route hosts. By default, the switch is not configured with any static routes. The syntax is: IP address / subnet.



Host Static Route Configuration

Target Address/Subnet perfix	Next Hop

Item	Target Address/Subnet perfix	Next Hop	Distance	State

CERTIFICATION. AUTHORIZATION. ACCOUNTING (AAA) CONFIGURATION

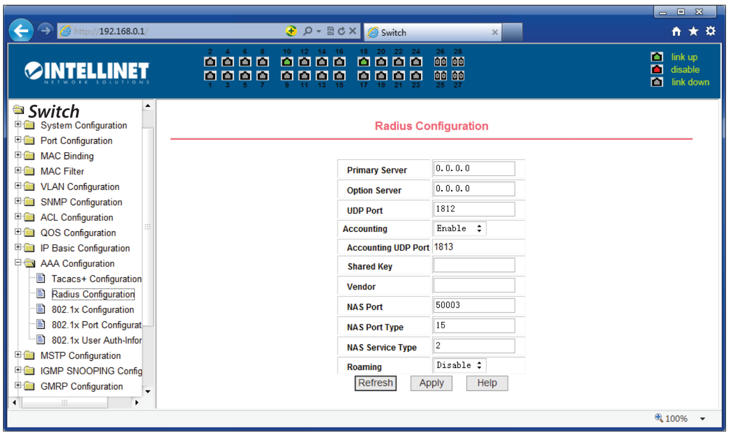
RADIUS CONFIGURATION

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. 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.

The following image shows the RADIUS Configuration page. From this screen it is possible to:

- Set the RADIUS server's IP address first.
- Add an optional RADIUS server IP address.
- Set the Authentication UDP port, the default value is 1812.
- Enable or disable Accounting.
- Set the Accounting UDP$^{\textit{Switch}}$ port, the default value is 1813.
- Set the shared secret key, which is used between the switch and the RADIUS server.
- Set the vendor-specific information if required.
- Set the NAS port, NAS port type and NAS type of service again if required.
- Enable or disable the roaming feature of RADIUS.



Radius Configuration

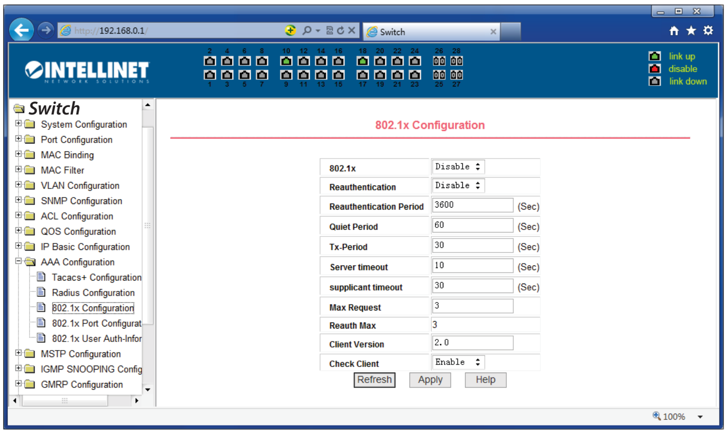
Primary Server	0.0.0.0
Option Server	0.0.0.0
UDP Port	1812
Accounting	Enable
Accounting UDP Port	1813
Shared Key	
Vendor	
NAS Port	50003
NAS Port Type	15
NAS Service Type	2
Roaming	Disable

802.1X CONFIGURATION

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.

The following image shows the 802.1x Configuration page. From this screen it is possible to:

- Enable or disable the 802.1x protocol, which is required when authentication and accounting are being implemented.
- Enable or disable Reauthentication, which increases network traffic when enabled.
- Set the Reauthentication period; the default is 3600 seconds.
- Set Quiet Period Timer, if required.
- Set Tx-Period Timer, if required.
- Set Server timeout timer, if required.
- Set Supplicant timeout timer, if required.
- Set Max Request number, if required.
- View Max Request value.
- Client Version, the client version number.
- Enable or disable Check



802.1x Configuration

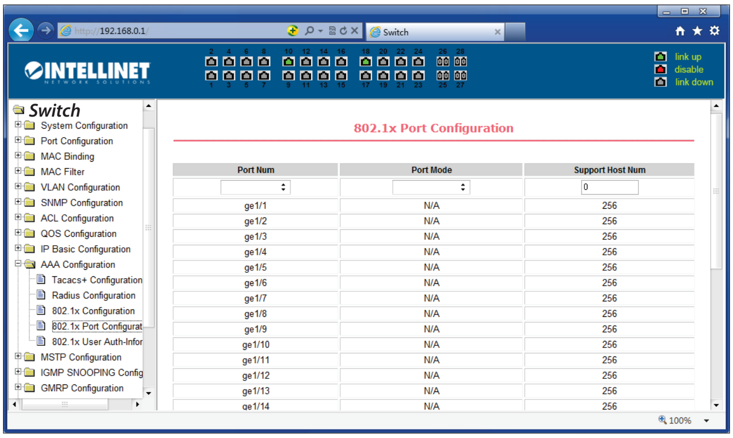
802.1x	Disable	
Reauthentication	Disable	
Reauthentication Period	3600	(Sec)
Quiet Period	60	(Sec)
Tx-Period	30	(Sec)
Server timeout	10	(Sec)
supplicant timeout	30	(Sec)
Max Request	3	
Reauth Max	3	
Client Version	2.0	
Check Client	Enable	

Refresh Apply Help

802.1X PORT CONFIGURATION

The following image shows the 802.1x Port Configuration page. From this screen it is possible to:

- View 802.1x port configuration.
- Set the state of the port to N/A, Auto, Force Authorization or Force Unauthorized state. (Generally N/A or Auto are used).
- Set the value for the maximum host number (The default value is 100).

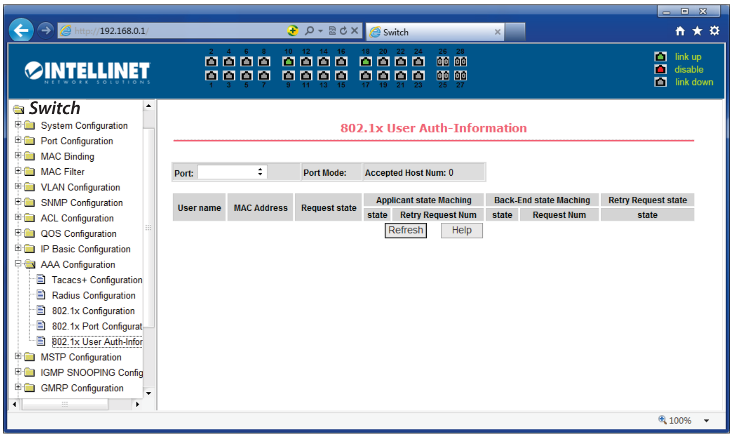


802.1x Port Configuration

Port Num	Port Mode	Support Host Num
		0
ge1/1	N/A	256
ge1/2	N/A	256
ge1/3	N/A	256
ge1/4	N/A	256
ge1/5	N/A	256
ge1/6	N/A	256
ge1/7	N/A	256
ge1/8	N/A	256
ge1/9	N/A	256
ge1/10	N/A	256
ge1/11	N/A	256
ge1/12	N/A	256
ge1/13	N/A	256
ge1/14	N/A	256

802.1X USER AUTHENTICATION INFORMATION

The following image shows the 802.1x user authentication information page, which displays the authentication data.



802.1x User Auth-Information

Port: Port Mode: Accepted Host Num: 0

User name	MAC Address	Request state	Applicant state Maching		Back-End state Maching		Retry Request state
			state	Retry Request Num	state	Request Num	state

Refresh Help

SPANNING TREE PROTOCOL CONFIGURATION

MSTP GLOBAL CONFIGURATION

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:

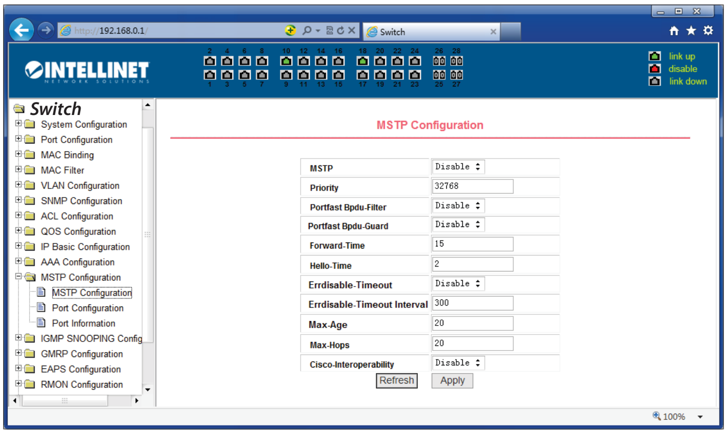
- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

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.

The following image shows the MSTP global configuration page. From this screen, it is possible to:

- Enable or disable MSTP.
- Configure the bridge priority. Devices with lower priority are more likely to be the root bridge.
- Enable or disable the BPDU filtering function on the port in the portfast bpdu-filter default state.
- Enable or disable the BPDU guard function on the port in the portfast bpdu-guard default state.
- Configure the forwarding delay.
- Configure the interval for sending MSTP Hello packets.
- Start the errdisable mechanism. When a port that starts a BPDU guard or receives a BPDU, it starts the errordisable timer. errordisable restarts this port after the configured timeout.
- Configure errordisable timeout time.
- Configure the number of seconds the switch waits to receive spanning tree configuration information before triggering a reconfiguration.
- Configure the number of hops specified before a BPDU is dropped in a domain.
- Start or shut down any Cisco-compatible spanning tree protocol.



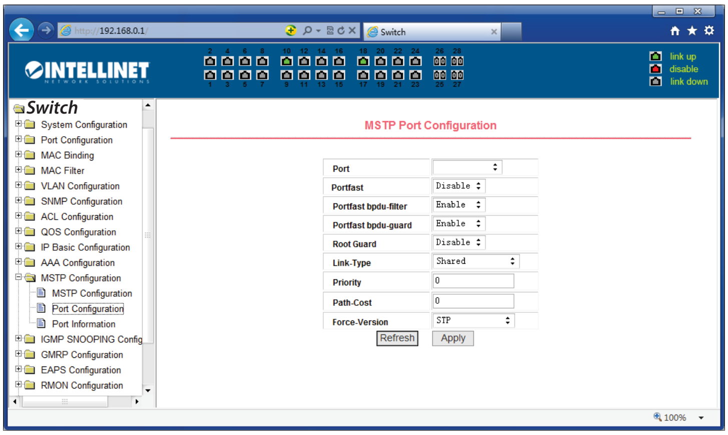
MSTP Configuration

MSTP	Disable
Priority	32768
Portfast Bpdu-Filter	Disable
Portfast Bpdu-Guard	Disable
Forward-Time	15
Hello-Time	2
Errdisable-Timeout	Disable
Errdisable-Timeout Interval	300
Max-Age	20
Max-Hops	20
Cisco-Interoperability	Disable

MSTP PORT CONFIGURATION

The following image shows the MSTP configuration page. Make MSTP-related configurations here, such as:

- Select the port to be configured.
- Configure a port as a portfast port to change the port from the blocking state to the forwarding state, bypassing the listening and learning states.
- Open the BPDU filter on the selected port.
- Enable BPDU guard on the selected port.
- Enable the root guard function, and do not accept BPDU packets with a higher priority than the bridge. Specify the switch as the root switch.
- Configure the connection type.
- Point-to-point: allows fast transition of the port status.
- Shared: does not allow rapid conversion of port status to go through the calculation process of 802.1D to determine the status of the port.
- Configure the cist priority of the interface. The range is from 0 – 240 and can only be a multiple of 16. The default is 128.
- Configure the cist path cost. The range is from 1 – 200000000. The default is 20000000. Lower-path costs are more likely to be roots.
- Configure the type of protocol packets to be sent.



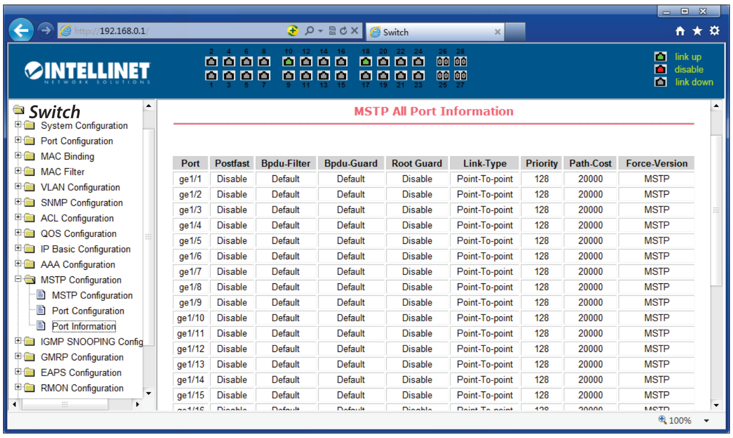
MSTP Port Configuration

Port	
Portfast	Disable
Portfast bpdu-filter	Enable
Portfast bpdu-guard	Enable
Root Guard	Disable
Link-Type	Shared
Priority	0
Path-Cost	0
Force-Version	STP

Refresh Apply

MSTP CONFIGURATION INFORMATION

The following image shows the MSTP configuration information page, through which you can view some MSTP related information.



MSTP All Port Information

Port	Postfast	Bpdu-Filter	Bpdu-Guard	Root Guard	Link-Type	Priority	Path-Cost	Force-Version
ge1/1	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/2	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/3	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/4	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/5	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/6	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/7	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/8	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/9	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/10	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/11	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/12	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/13	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/14	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/15	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/16	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

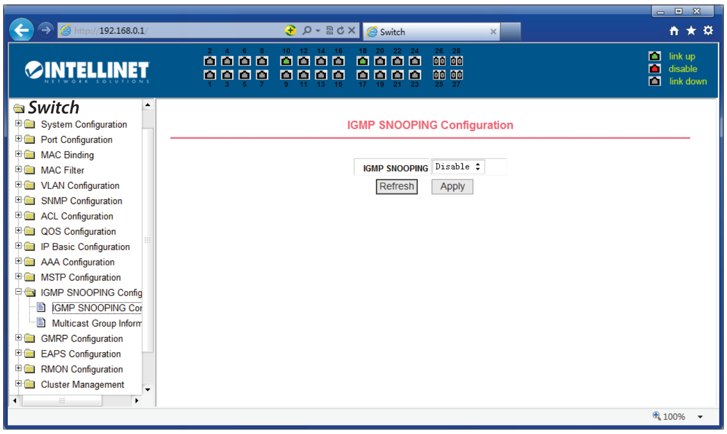
IGMP SNOOPING CONFIGURATION

IGMP SNOOPING CONFIGURATION

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.

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. Using IGMP, the router can check to see if there is at least one member of a multicast group on a given sub network. If there are no members on a sub network, packets will not be forwarded to that sub network.

The following image shows the IGMP Snooping configuration page, through which you can start this function.

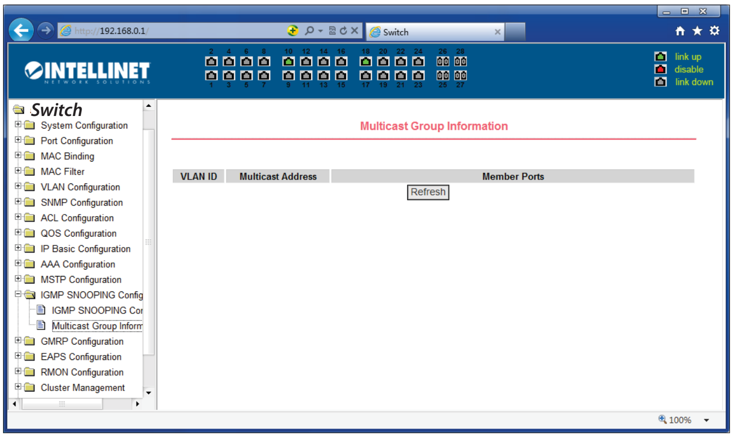


IGMP SNOOPING Configuration

IGMP SNOOPING: Disable

IGMP SNOOPING INFORMATION

The following image shows the IGMP Snooping information page, which allows users to view some information about IGMP Snooping.



Multicast Group Information

VLAN ID	Multicast Address	Member Ports

GMRP CONFIGURATION

GMRP GLOBAL CONFIGURATION

The following sections describe how to configure the GARP Multicast Registration Protocol (GMRP).

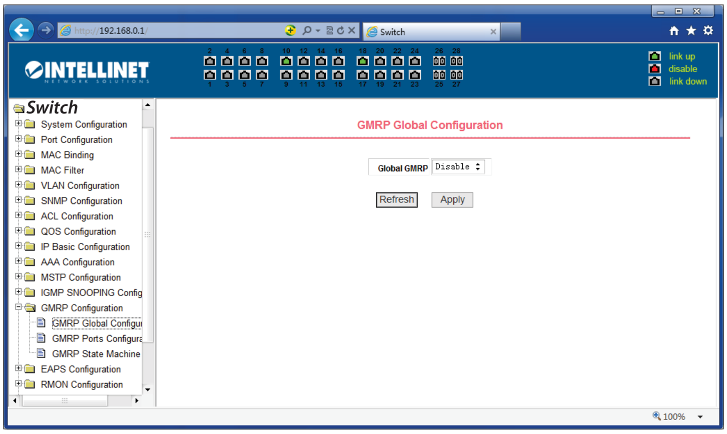
GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping. GMRP and GARP are industry-standard protocols defined by the IEEE 802.1P.

GMRP provides a mechanism that allows bridges and end stations to dynamically register group membership information with the MAC bridges attached to the same LAN segment and for that information to be disseminated across all bridges in the Bridged LAN that supports extended filtering services. The operation of GMRP relies upon the services provided by the GARP.

GMRP software components run on both the switch and on the host. On the host, GMRP is typically used with IGMP: the host GMRP software spawns Layer 2 GMRP versions of the host's Layer 3 IGMP control packets. The switch receives both the Layer 2 GMRP and the Layer 3 IGMP traffic from the host. The switch uses the received GMRP traffic to constrain multicasts at Layer 2 in the host’s VLAN. In all cases, you can use IGMP snooping to constrain multicasts at Layer 2 without the need to install or configure software on hosts.

When a host wants to join an IP multicast group, it sends an IGMP join message, which spawns a GMRP join message. Upon receipt of the GMRP join message, the switch adds the port through which the join message was received to the appropriate Multicast group. The switch propagates the GMRP join message to all other hosts in the VLAN, one of which is typically the Multicast source. When the source is multicasting to the group, the switch forwards the multicast only to the ports from which it received join messages for the group. The switch sends periodic GMRP queries. If a host wants to remain in a multicast group, it responds to the query. In this case, the switch does nothing. If a host does not want to remain in the Multicast group, it can either send a leave message or not respond to the periodic queries from the switch. If the switch receives a leave message or receives no response from the host for the duration of the leave all timer, the switch removes the host from the multicast group.

The following image shows the GMRP global configuration page.

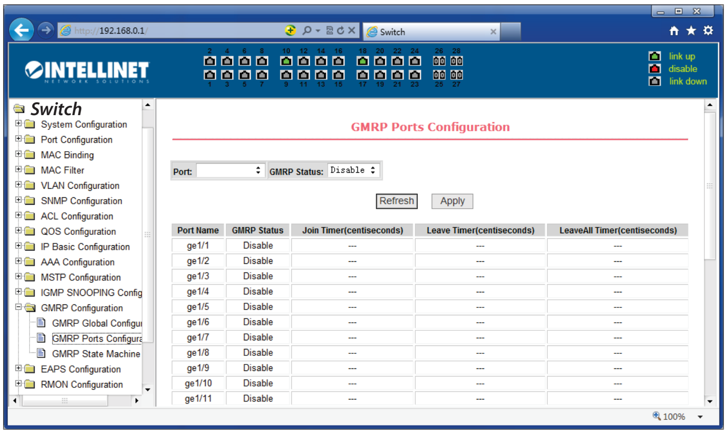


GMRP Global Configuration

Global GMRP: Disable

GMRP PORTS CONFIGURATION

The following image shows the GMRP port configuration page. Use this page to enable the GMRP port and view the port information.



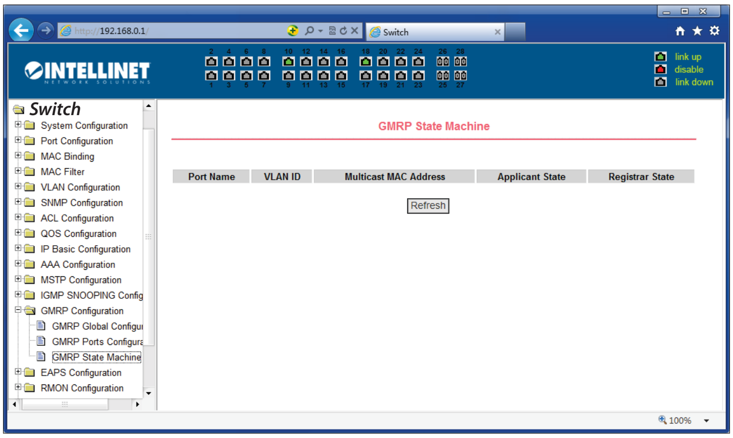
GMRP Ports Configuration

Port: GMRP Status: Disable

Port Name	GMRP Status	Join Timer(centiseconds)	Leave Timer(centiseconds)	LeaveAll Timer(centiseconds)
ge1/1	Disable	---	---	---
ge1/2	Disable	---	---	---
ge1/3	Disable	---	---	---
ge1/4	Disable	---	---	---
ge1/5	Disable	---	---	---
ge1/6	Disable	---	---	---
ge1/7	Disable	---	---	---
ge1/8	Disable	---	---	---
ge1/9	Disable	---	---	---
ge1/10	Disable	---	---	---
ge1/11	Disable	---	---	---

GMRP STATE MACHINE

The following image shows the GMRP state machine page. Users can view the GMRP state machine information here.



GMRP State Machine

Port Name	VLAN ID	Multicast MAC Address	Applicant State	Registrar State

EAPS CONFIGURATION

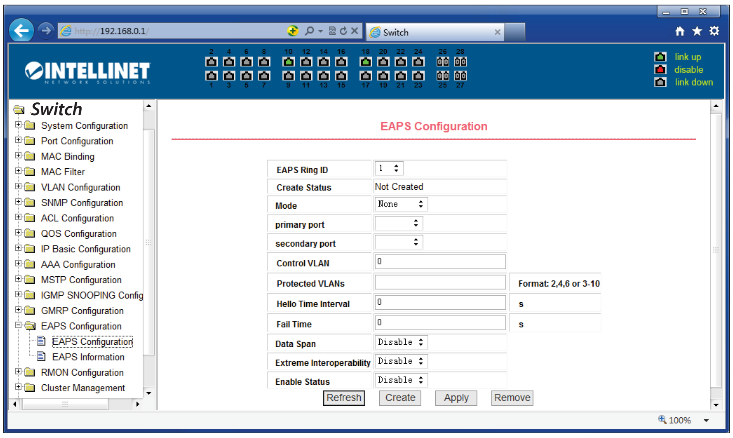
Ethernet Automatic Protection Switching (EAPS) is used to create a fault tolerant topology by configuring a primary and secondary path for each VLAN. A ring is formed by configuring a Domain. Each domain has a single "master node" and many "transit nodes". Each node will have a primary port and a secondary port, both known to be able to send control traffic to the master node. Under normal operation, the secondary port on the master is blocked for all protected VLANs. When a link is down, the devices that detect the failure send a control message to the master, and the master will then unblock the secondary port and instruct the transits to flush their forwarding databases. The next packets sent by the network can then be flooded and learned out of the (now enabled) secondary port without any network disruption.

The same switch can belong to multiple domains and thus multiple rings. However, these act as independent entities and can be controlled individually.

EAPS CONFIGURATION

The image on the next page shows an EAPS configuration page, through which you can configure some EAPS related information, including:

- Select an EAPS ring number.
- Configure the operating node mode of an EAPS Domain.
- Configure Primary Port of EAPS Domain.
- Configure Secondary Port of EAPS Domain.
- Configure a control VLAN for EAPS Domain.
- Add one or more protected VLANs of the EAPS Domain.
- Configure an EAPS Domain to periodically send HEALTH packets. Hello-timer must be less than fail-time.
- Set the fail-period timer of one EAPS domain to expire.
- Enable or disable compatibility with Extreme devices.
- Whether to enable



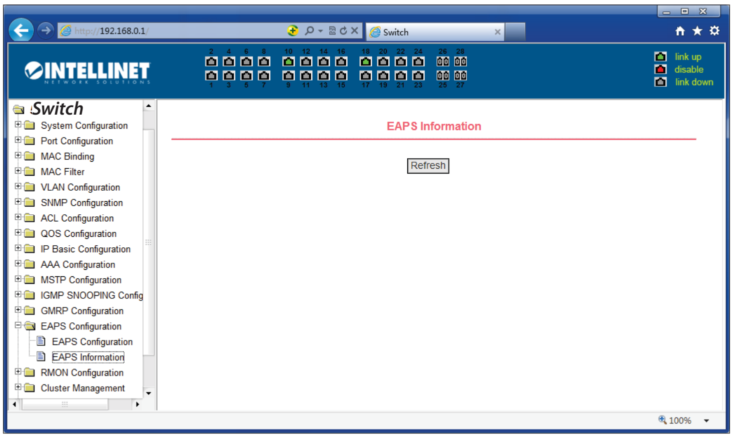
EAPS Configuration

EAPS Ring ID	1	
Create Status	Not Created	
Mode	None	
primary port		
secondary port		
Control VLAN	0	
Protected VLANs		Format: 2,4,6 or 3-10
Hello Time Interval	0	s
Fail Time	0	s
Data Span	Disable	
Extreme Interoperability	Disable	
Enable Status	Disable	

Refresh Create Apply Remove

EAPS INFORMATION

The following image shows an EAPS information page, through which users can view some EAPS related information.



EAPS Information

Refresh

RMON CONFIGURATION

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.

MIB of RMON consists of 10 groups. The Switch supports the most frequently used groups 1, 2, 3 and 9:

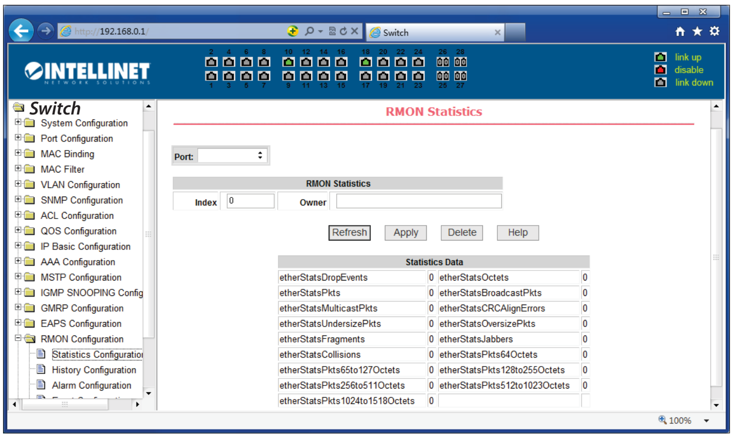
- Statistics: Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface.
- History: Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.
- Alarm: Monitors a specific MIB object for a specified interval, 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 MIB in RFC1757 as an extension of the SNMP.

RMON STATISTICS GROUP CONFIGURATION

The following image shows the RMON statistics group configuration page.

Select a port from the drop-down list to view/configure the RMON statistics group configuration for this port. When not configured, the index number is 0. Fill in the index number (range 1 to 100); the owner is optional. The statistics table shows the port statistics after successful configuration.



RMON Statistics

Port:

RMON Statistics			
Index	0	Owner	

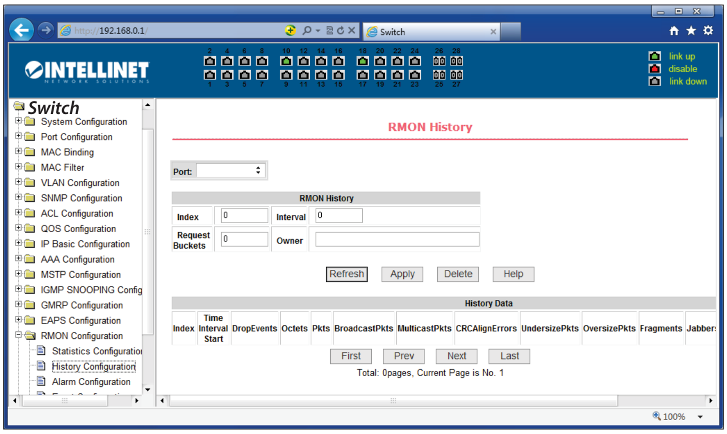
Statistics Data			
etherStatsDropEvents	0	etherStatsOctets	0
etherStatsPkts	0	etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0	etherStatsCRCAlignErrors	0
etherStatsUndersizePkts	0	etherStatsOversizePkts	0
etherStatsFragments	0	etherStatsJabbers	0
etherStatsCollisions	0	etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0	etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0	etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0		

RMON HISTORY GROUP CONFIGURATION

The following image shows the RMON history group configuration page.

Select a port from the drop-down list to view/configure the RMON history group configuration for this port. When not configured, the index number is 0. Fill in the index number (range is 1 to 100), interval, request buckets; the owner is optional.

Interval refers to the time interval in seconds that the data is collected. The range is 1-3600. The bucket is the allocated storage size, and it indicates how many records are stored. The range is 1-100. The statistics table shows historical data that has been collected since the configuration was successful.



RMON History

Port:

RMON History			
Index	0	Interval	0
Request Buckets	0	Owner	

History Data

Index	Time Interval Start	DropEvents	Octets	Pkts	BroadcastPkts	MulticastPkts	CRCAlignErrors	UndersizePkts	OversizePkts	Fragments	Jabber:

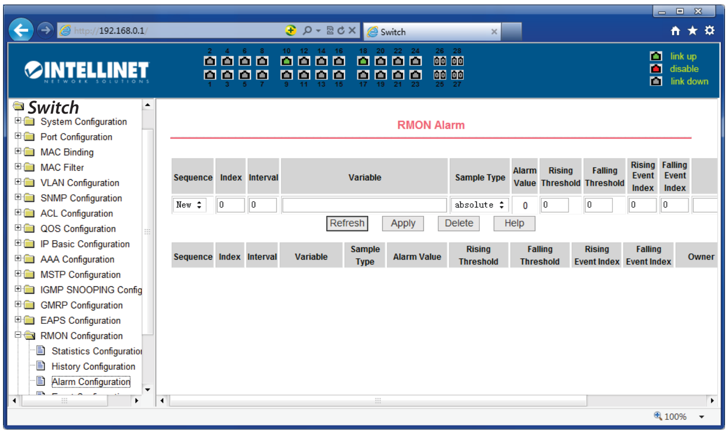
Total: 0pages, Current Page is No. 1

RMON ALARM GROUP CONFIGURATION

The image on the next page shows the RMON alarm group configuration page. From this page, you can:

- Select a configured alarm group from the drop-down list to view/configure its information.
- Select New to create an alarm group: the index number range is from 1 to 60, and the interval range is from 1 to 3600 (In seconds). In the variable field specify the MIB that is monitored by the alarm entry. The comparison method can be absolute or delta.

   - The alarm value is read-only and shows the sampled value when the alarm was last issued. The rising threshold shows a number at which the alarm is triggered. This value ranges between 0 and 2147483647.
   - The falling threshold, a number at which the alarm is reset. This value ranges between 0 and 2147483647.
- Value, event index and owner are optional.
- The event index refers to the index number of the RMON event group and must be configured in advance.



RMON Alarm

Sequence	Index	Interval	Variable	Sample Type	Alarm Value	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	
New	0	0		absolute	0	0	0	0	0	

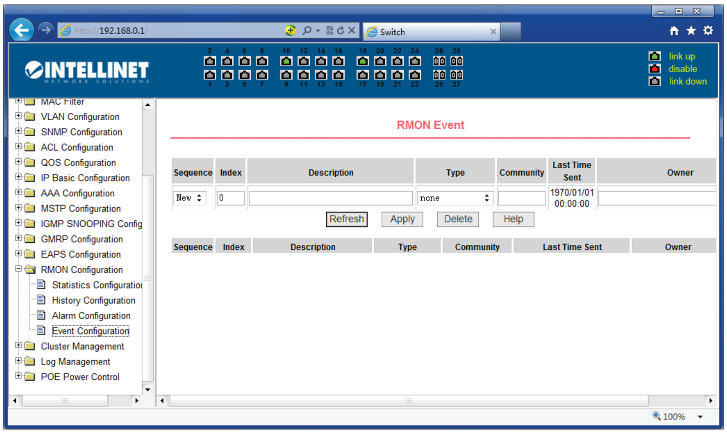
Sequence	Index	Interval	Variable	Sample Type	Alarm Value	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner

RMON EVENT GROUP CONFIGURATION

The following image shows the RMON event group configuration page.

Select a configured event group from the drop-down list to view/configure its information. Select New to create one.

- The index number range is from 1 to 60.
- The description is a character string.
- Type can be one of:
   - none (no operation)
   - log (log)
   - snmp-trap (trap trap)
   - log-and-trap (log and trap alarm)
   - Community names are not required.
   - Owner is optional.
   - The Last Time Sent is read-only, showing the last time the event was sent.



RMON Event

Sequence	Index	Description	Type	Community	Last Time Sent	Owner
New	0		none		1970/01/01 00:00:00	

Sequence	Index	Description	Type	Community	Last Time Sent	Owner

CLUSTER CONFIGURATION

Neighbor Discovery Protocol (NDP) is an important protocol in IPv6. NDP is based on ICMPv6 and is used to identify the relationships between different neighboring devices in an IPv6 network. Many important functions of IPv6 such as resolving MAC address of an IPv6 Address (in IPv4, ARP is used for this), Router Discovery etc., are now performed using Neighbor Discovery Protocol (NDP).

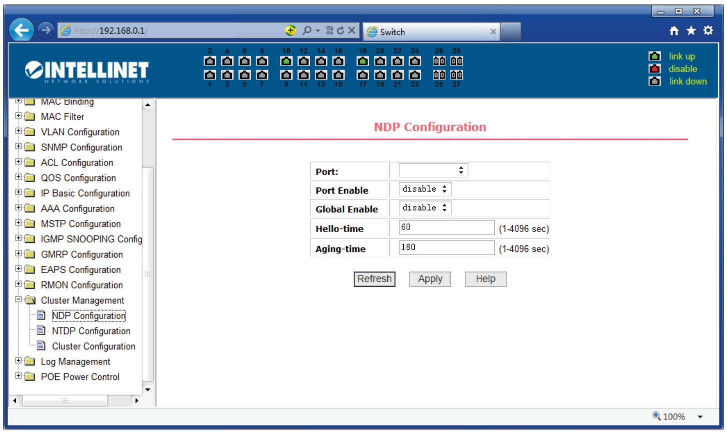
The following are the important functions of Neighbor Discovery Protocol (NDP):

- **Discovering Routers Dynamically:** NDP is used to automatically discover routers in an IPv6 network using Router Solicitation & Router Advertisement messages.
- **Discovering Network Prefixes Dynamically:** NDP is used to automatically discover IPv6 network prefixes where the host belongs to, by using Router Solicitation & Router Advertisement messages.
- **Resolving MAC address dynamically:** We use IP addresses for communication but the addresses which are used by the LAN Switches for delivery of Ethernet frames to the destination devices are MAC addresses. In IPv4, Address Resolution Protocol (ARP) is used for resolving IPv4 address to MAC address. The role of ARP in IPv4 is performed by NDP in IPv6.
- **Autoconfiguration of IPv6 addresses:** After learning IPv6 network prefixes using NDP Router Solicitation & Router Advertisement messages, IPv6 devices can autoconfigure an IPv6 address by self-generating the host part of the IPv6 address by using EUI-64 method.
- **DAD (Duplicate Address Detection):** DAD is an NDP mechanism to detect whether duplicate IPv6 addresses exist in an IPv6 network. DAD is useful because IPv6 has many address autoconfiguration mechanisms.

NDP CONFIGURATION

The following image shows the NDP configuration page.

- The configurable information includes:
- Selecting the port (for port selection, select the port as required, and enable the port NDP function)
- Enabling the NDP function of the port For NDP (both global and port NDP must be enabled)
- Enabling the global NDP function (both global and port NDP must be enabled)
- Entering the interval for sending NDP packets (the valid time range is 1-4096 seconds; the default value is 180 seconds)
- Entering the aging time of the NDP packets on the receiving device (the valid time range is 1-4096 seconds, and the default is 60 seconds)



NDP Configuration

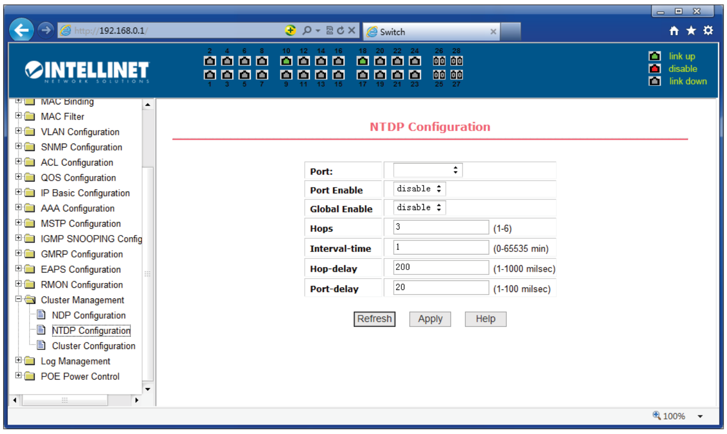
Port:	
Port Enable	disable
Global Enable	disable
Hello-time	60 (1-4096 sec)
Aging-time	180 (1-4096 sec)

NTDP CONFIGURATION

The following image shows the NTDP configuration page.

The information that can be set includes:

- Selecting the port (for port selection, select the port as required and enable the port NDP function)
- Enabling the NTDP function of the port (both global and port NDP must be enabled)
- Enabling the global NTDP function (both global and port NDP must be enabled)
- Entering the range of the topology collection (range is 1 – 6; the default is 3)
- Entering the time interval of collecting the regular topology (range is 0 – 65535 minutes; the default is 1 minute)
- Entering the delay time of the first port forwarding the packet (range is 1 – 1000 milliseconds; the default is 200 milliseconds)
- Entering the forwarding of the packet by other ports (range is 1 – 100 milliseconds; the default is 20 milliseconds)



NTDP Configuration

Port:		
Port Enable	disable	
Global Enable	disable	
Hops	3	(1-6)
Interval-time	1	(0-65535 min)
Hop-delay	200	(1-1000 milsec)
Port-delay	20	(1-100 milsec)

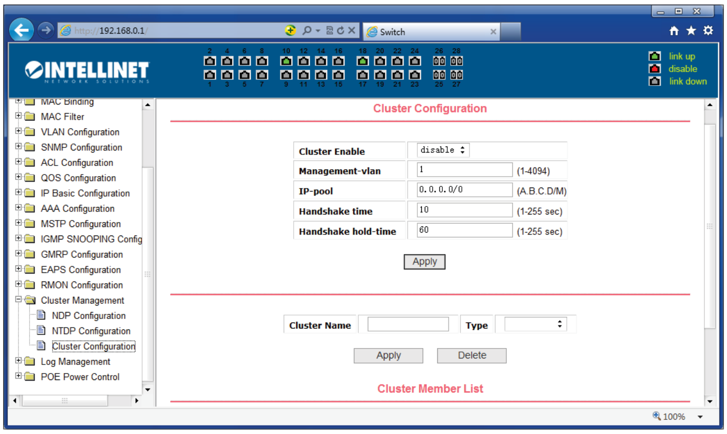
Refresh Apply Help

CLUSTER CONFIGURATION

The following image shows the cluster configuration page. The information that can be set includes:

- Enabling the cluster function
- Configuring the management VLAN (range is 1 – 4094; the default is vlan1)
- Entering the address pool of the cluster (range of IP addresses is 0.0.0.0 – 255.255.255.255; range of the mask length is 0 – 32)
- Entering the interval for sending handshake packets (range is 1 – 255 seconds; the default is 10 seconds)
- Entering the effective retention time of the device (range is 1 – 255 seconds; the default is 60 seconds)
- Entering the name of the cluster (self-explanatory)
- Entering the way to join the cluster (manual or automatically)

After a cluster is established, member devices and candidate devices can be viewed in the cluster member table. You can delete member devices or add candidate devices to member devices according to roles.



Cluster Configuration

Cluster Enable	disable	
Management-vlan	1	(1-4094)
IP-pool	0.0.0.0/0	(A.B.C.D/M)
Handshake time	10	(1-255 sec)
Handshake hold-time	60	(1-255 sec)

Apply

Cluster Name Type

Apply Delete

Cluster Member List

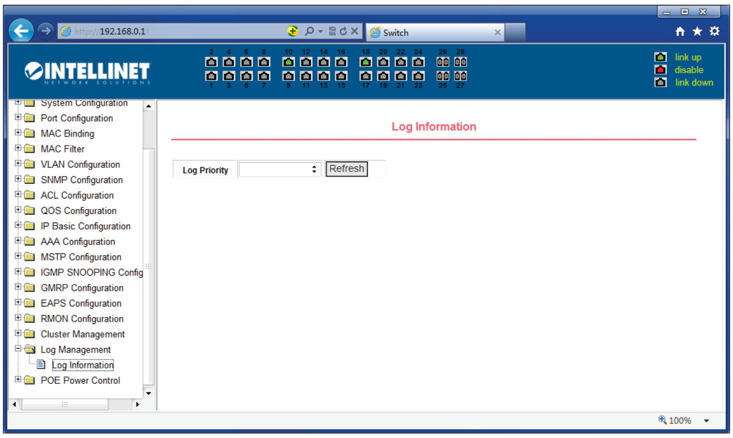
LOG MANAGEMENT

LOG INFORMATION

The following image shows the Log Information page. Users can enable and view various log information through this page.

Configurable options are as follows:

- **Critical**: outputs critical level information
- **Debugging**: outputs debug level information
- **Informational**: output information-level debugging data
- **Warning**: outputs warning-level debugging information
- **All**: outputs all log information



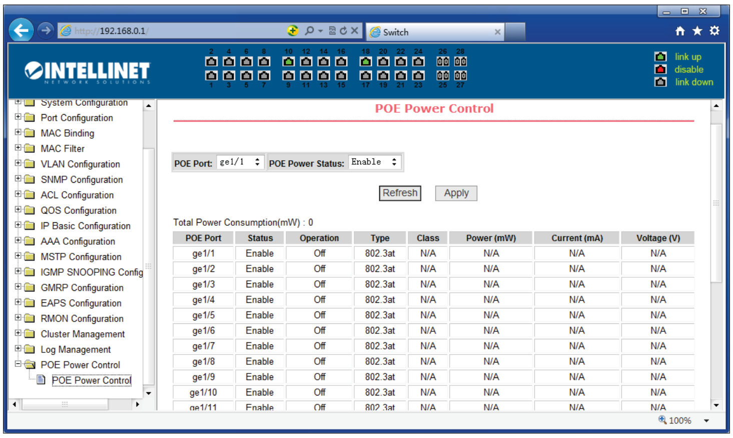
Log Information

Log Priority Refresh

POE POWER CONTROL

POE PORT CONFIGURATION

The following image shows the PoE Port Configuration page, which allows users to enable or disable PoE on each port and view the status of PoE on a per port basis (mW, mA and Voltage). This page also lets users view the total power consumption and see the type and class of PoE on a per port basis.



POE Power Control

POE Port: ge1/1 POE Power Status: Enable

Total Power Consumption(mW) : 0

POE Port	Status	Operation	Type	Class	Power (mW)	Current (mA)	Voltage (V)
ge1/1	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/2	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/3	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/4	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/5	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/6	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/7	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/8	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/9	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/10	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/11	Enable	Off	802.3at	N/A	N/A	N/A	N/A

ADDITIONAL INFORMATION

WASTE ELECTRICAL & ELECTRONIC EQUIPMENT

DISPOSAL OF ELECTRIC AND ELECTRONIC EQUIPMENT

(Applicable In The European Union And Other European Countries With Separate Collection Systems)

ENGLISH: This symbol on the product or its packaging means that this product must not be treated as unsorted household waste. In accordance with EU Directive 2012/19/EU on Waste Electrical and Electronic Equipment (WEEE), this electrical product must be disposed of in accordance with the user's local regulations for electrical or electronic waste. Please dispose of this product by returning it to your local point of sale or recycling pickup point in your municipality.

DEUTSCH: Dieses auf dem Produkt oder der Verpackung angebrachte Symbol zeigt an, dass dieses Produkt nicht mit dem Hausmüll entsorgtwerden darf. In Übereinstimmung mit der Richtlinie 2012/19/EU des Europäischen Parlaments und des Rates über Elektro- und Elektronik-Altgeräte (WEEE) darf dieses Elektrogerät nicht im normalen Hausmüll oder dem Gelben Sack entsorgt werden. Wenn Sie dieses Produkt entsorgen möchten, bringen Sie es bitte zur Verkaufsstelle zurück oder zum Recycling-Sammelpunkt Ihrer Gemeinde.

ESPAÑOL: Este símbolo en el producto o su embalaje indica que el producto no debe tratarse como residuo doméstico. De conformidad con la Directiva 2012/19/EU de la UE sobre residuos de aparatos eléctricos y electrónicos (RAEE), este producto eléctrico no puede desecharse se con el resto de residuos no clasificados. Deshágase de este producto devolviéndolo a su punto de venta o a un punto de recolección municipal para su reciclaje.

FRANÇAIS: Ce symbole sur le produit ou son emballage signifie que ce produit ne doit pas être traité comme un déchet ménager. Conformément à la Directive 2012/19/EU sur les déchets d'équipements électriques et électroniques (DEEE), ce produit électrique ne doit en aucun cas être mis au rebut sous forme de déchet municipal non trié. Veuillez vous débarrasser de ce produit en le renvoyant à son point de vente ou au point de ramassage local dans votre municipalité, à des fins de recyclage.

ITALIANO: Questo simbolo sui prodotto o sulla relativa confezione indica che il prodotto non va trattato come un rifiuto domestico. In ottemperanza alla Direttiva UE 2012/19/EU sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE), questa prodotto elettrico non deve essere smaltito come rifiuto municipale misto. Si prega di smaltire il prodotto riportandolo al punto vendita o al punto di raccolta municipale locale per un opportuno riciclaggio.

POLSKI: Jeśli na produkcie lub jego opakowaniu umieszczono ten symbol, wówczas w czasie utylizacji nie wolno wyrzucać tego produktu wraz z odpadami komunalnymi. Zgodnie z Dyrektywą Nr 2012/19/EU w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE), niniejszego produktu elektrycznego nie wolno usuwać jako nie posortowanego odpadu komunalnego. Prosimy o usuniecie niniejszego produktu poprzez jego zwrot do punktu zakupu lub oddanie do miejscowego komunalnego punktu zbiórki odpadów przeznaczonych do recyklingu.

WARRANTY INFORMATION • GARANTIEINFORMATIONEN • GARANTÍA • GARANTIE • GWARANCJI • GARANZIA

USA & CANADA: intellinetsolutions.com
EUROPE: intellinetnetwork.eu
DEUTSCHLAND: intellinetnetwork.de
EN MÉXICO: intellinetsolutions.mx

EN MÉXICO: Póliza de Garantía Intellinet Network Solutions — 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, Cuautitlán 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 los productos de limpieza, aire comprimido y consumibles, por 60 dias a partir de la fecha de entrega, o por el tiempo en que se agote totalmente su contenido por su propia función de uso, lo que suceda primero.

B. Garantizamos los productos con partes móviles por 3 años.

C. 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.

REGULATORY STATEMENTS

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of Federal Communications Commission (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: reorient or relocate the receiving antenna; increase the separation between the equipment and the receiver; connect the equipment to an outlet on a circuit different from the receiver; or consult the dealer or an experienced radio/TV technician for help.

CE

ENGLISH: This device complies with the requirements of CE RED 2014/53/EU, 2014/30/EU and/or 2014/35/EC. The Declaration of Conformity for is available at:

DEUTSCH: Dieses Gerät enspricht der CE RED 2014/53/EU, 2014/30/EU und / oder 2014/35/EC. Die Konformitätserklärung für dieses Produkt finden Sie unter:

ESPAÑOL: Este dispositivo cumple con los requerimientos de CE RED 2014/53/EU, 2014/30/EU y / o 2014/35/EC. La declaración de conformidad esta disponible en:

FRANÇAIS: Cet appareil satisfait aux exigences de CE RED 2014/53/EU, 2014/30/EU et / ou 2014/35/EC. La Déclaration de Conformité est disponible à:

POLSKI: Urządzenie spełnia wymagania CE RED 2014/53/EU, 2014/30/EU I / lub 2014/35/EC. Deklaracja zgodności dostępna jest na stronie internetowej producenta:

ITALIANO: Questo dispositivo è conforme alla CE RED 2014/53/EU, 2014/30/EU e / o 2014/35/EC. La dichiarazione di conformità è disponibile al:

intellinetsolutions.com

North America
IC Intracom America
550 Commerce Blvd.
Oldsmar, FL 34677 USA

Asia & Africa
IC Intracom Asia
4-F, No. 77, Sec. 1, Xintai 5th Rd.
Xizhi Dist., New Taipei City 221, Taiwan

Europe
IC Intracom Europe
Löhbacher Str. 7, D-58553
Halver, Germany

INTELLINET®
NETWORK SOLUTIONS

intellinetsolutions.com