



# **XikeStor L2 Managed Switch**

## **Web Management User Manual**

**(Take SKS7300-12GPY2XGT2XGS as an example)**



## Catalogue

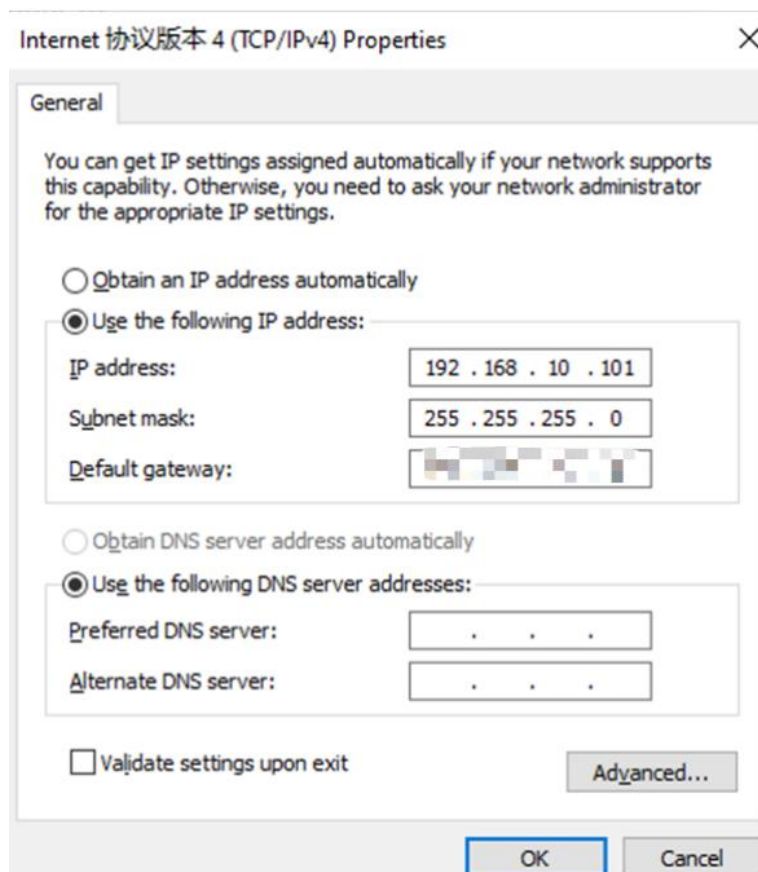
1. Accessing the Switch and Logging in Using a Web Browser .....	2
(1) To log into the switch using browser-based access .....	1
2. System Management .....	3
(1) Modify the Switch Management IP Address .....	3
(2) Modification Over Time .....	4
(3) System Time .....	5
(4) Save Settings .....	8
(5) SNMP Management .....	8
3. L2 Switching Management .....	9
(1) Port Management .....	9
(2) Convergence Group Management .....	10
(3) VLAN Management .....	11
(4) MAC Management .....	14
4. Security Management .....	15
(1) Add New User .....	15
(2) Setting the ACL .....	15
(3) Port Isolation .....	16
5. Monitoring Management .....	16
(1) Port Information .....	16
(2) Mirror Management .....	16
6. Maintenance .....	19
(1) Save Settings .....	19
(2) Reboot .....	19
(3) Download Configuration File .....	20
(4) Updating Device Files .....	20
(5) IMG Document Management .....	21
(6) Diagnostic Tool .....	21

# 1. Accessing the Switch and Logging in Using a Web Browser

You can use a web browser to access the switch and log in to configure it. You must be able to successfully ping the IP address of the managed switch's management interface from the management system before you can begin using web access to.

(1) To log into the switch using browser-based access

First of all, plug the computer with a network cable into any one of the switch's network ports (not into the yellow console management port), and then set the computer's IP address and the switch's default IP address into a network segment, for example, 192.168.10.101, and refer to the picture for the subnet mask and the default gateway, and then click on Confirm. Refer to the following picture to set:



Open your computer browser, Firefox or Google Chrome is recommended, enter the IP address of the switch in the browser, the default IP address of the switch is 192.168.10.12. The login screen will be displayed, enter the default user name and password. The default administrator username



is admin and the default administrator password is empty, i.e. do not enter a password. Click the Login button to enter the management interface of the switch.

**SKS7300-12GPY2XGT2XGS**  
**Management Login**

	<b>User ID</b>	<input type="text" value="admin"/>
	<b>Password</b>	<input type="password"/>
		<input type="button" value="Login"/> <input type="button" value="Cancel"/>

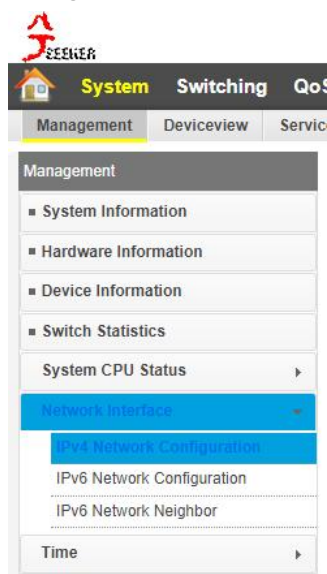
## 2. System Management

In the System Management - Basic Management interface, you can see some basic information and operation information of the switch.

Because there are many functions of the switch, this tutorial will not list them all, but only list the relatively more commonly used functions to do a detailed introduction.

### (2) Modify the Switch Management IP Address

After logging in go to Management - Management - Network Interface - IPv4 Network Configuration



All ports of the switch belong to VLAN1 by default, enter 1 in the management VLANID in the network band (the default is 1), the configuration mode can choose to configure manually, Bootp or DHCP (automatic acquisition), the default is manual configuration. Then enter the management interface IP address to be modified into the management IP, can be changed to your current network segment, so that you can enter directly through the browser later, our network segment for the 10.0.0 network segment, then I would distance to modify the 10.0.0.177, other places do not have to modify, so that later directly in the computer browser to enter this ip address, you can enter the management interface. Convenient for you to use later. You also need to enter the corresponding subnet mask in the management interface MASK value. Value (MASK value 255.255.255.0 generally do not need to modify, the specific calculation method can consult the relevant information and then modify, it is recommended to use the online ip calculator to calculate their own)



The screenshot shows the 'IPv4 Network Configuration - Inbound' page in the XikeStor web interface. The left sidebar contains a 'Management' menu with options like System Information, Hardware Information, Device Information, Switch Statistics, System CPU Status, Network Interface, IPv4 Network Configuration (selected), IPv6 Network Configuration, IPv6 Network Neighbor, and Time. The main content area displays the following configuration fields:

Management VLAN ID	1
Current Network Configuration Protocol	<input checked="" type="radio"/> None <input type="radio"/> Bootp <input type="radio"/> DHCP
IP Address	10.0.0.177
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Burned In MAC Address	30:52:5A:11:91:B0
Locally Administered MAC Address	00:00:00:00:00:00
MAC Address Type	<input checked="" type="radio"/> Burned In <input type="radio"/> Locally Administered
DHCP Vendor Class Identifier	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DHCP Vendor Class Identifier String	
Interface Status	Up

Since the switch is without built-in battery, please save manually after any configuration is completed, otherwise **the settings will be lost after power failure**. The save method is as follows, remember to always click save after changing any configuration.

The screenshot shows the 'Device View' page in the XikeStor web interface. The top navigation bar includes 'System', 'Switching', 'QoS', 'Security', 'Monitoring', and 'Maintenance'. The 'Device View' page displays a grid of 16 ports (1-16) and a 'com' port. The 'Save' button in the top right corner is highlighted with a red box.

### (3) Modification Over Time

In System Information - Switch Status, you can modify the timeout time of the web page in Login Timeout, i.e., the web page will need to be logged in again if no operation is performed beyond this time.

**SKS7300-12GPY2XGT2XGS**

English Save Logout

Management Deviceview Services DNS SNMP LLDP ISDP Timer Schedule

Management

- System Information
- Hardware Information
- Device Information
- Switch Statistics
- System CPU Status
- Network Interface
- Time

Apply Refresh

### System Information - Switch Status

Product Name	SKS7300-12GPY2XGT2XGS, 1.0.1.4
System Name	<input type="text"/> (Max:255 characters)
System Location	<input type="text"/> (Max:255 characters)
System Contact	<input type="text"/> (Max:255 characters)
Login Timeout	<input type="text" value="5"/> (0 to 60 minutes)
Management VLAN ID	1
IPv4 Network Interface	<a href="#">192.168.10.12/255.255.255.0</a>
IPv6 Network Interface	<a href="#">fe80::3252:5aff:fe11:91b0</a>
System Mac Address	30:52:5A:11:91:B0
L2 MAC Address	30:52:5A:11:91:B2
L3 MAC Address	30:52:5A:11:91:B3
System SNMP OID	1.3.6.1.4.1.4413
System Date	01/01/1970 00:13:40 (UTC+0:00)
System Up Time	13 minutes, 40 seconds
Current SNTP Sync Status	Fail or Not Start
Current SNTP synchronized Time	SNTP Client Mode is Disabled

### System Information - Device Status

Devices ID	1
Operational Code Image File Name	NOSRTM_1.0.1.4-B5_20230605
Firmware Version	1.0.1.4
Firmware Time Stamp	Mon Jun 5 02:01:14 2023 (GMT)
Serial Number	SKS730023110028
Certification	OK_0123350286A40D87EE-093013898

#### (4) System Time

##### ① Manual Configuration

Here it is recommended to check Automatically get time from browser.

However, note that this way will lose the system time 00 after a power failure, even if it is saved, so if you are in a position to do so, you can use the SNTP server below to get the time.

**SKS7300-12GPY2XGT2XGS**

English Save Logout

Management Deviceview Services DNS SNMP LLDP ISDP Timer Schedule

Management

- System Information
- Hardware Information
- Device Information
- Switch Statistics
- System CPU Status
- Network Interface
- Time
- SNTP Global Configuration
- SNTP Server Configuration
- DayLight Saving Configuration

Apply Refresh

### Time Configuration - Configuration

Clock Source	<input checked="" type="radio"/> Local <input type="radio"/> SNTP
	<input checked="" type="checkbox"/> Auto read form Web Browser
Date	<input type="text" value="03/08/2024"/> (MM/DD/YYYY)
Time	<input type="text" value="17:55:41"/> (HH:MM:SS)
Time Zone Name	<input type="text"/>
Offset Hours	<input type="text" value="0"/> (-12 to 13)
Offset Minutes	<input type="text" value="0"/> (0 to 59)
Time Zone Reference	<input type="text"/>

It is recommended that you check the box to automatically get the time from your browser



## ② Setting up SNTP

First enable SNTP to get the time.

The screenshot shows the 'Time Configuration - Configuration' page in the XikeStor web interface. The 'Clock Source' is set to 'SNTP'. The 'Date' is 03/08/2024 and the 'Time' is 17:57:06. The 'Apply' button is highlighted with a red arrow.

Then configure the SNTP server of the switch in SNTP Server Configuration, the server type usually selects IPv4, and the server address is entered as the IP address of the SNTP server. If DNS is selected for the server type, enter the domain name of the SNTP server for the server address. The last three items do not need to be filled in.

Fill it out and click Add.

The screenshot shows the 'SNTP Server Configuration - Configuration' page. The 'Server Type' is set to 'IPv4' and the 'Address' is 192.168.10.12. The 'Add' button is highlighted with a red arrow. A red box highlights the 'Port', 'Priority', and 'Version' fields with the text 'No need to enter these three items'.

Because we are located in the UTC+8 timezone, we need to set the timezone offset to 8 hours. This includes the option to set the offset in minutes for even more accurate timekeeping

SKS7300-12GPY2XGT2XGS

System Switching QoS Security Monitoring Maintenance English Save Logout

Management Deviceview Services DNS SNMP LLDP ISDP Timer Schedule

**Management**

- System Information
- Hardware Information
- Device Information
- Switch Statistics
- System CPU Status
- Network Interface
- Time**
- Time Configuration
- SNTP Global Configuration
- SNTP Server Configuration
- DayLight Saving Configuration

Time Configuration - Configuration

Apply Refresh

Clock Source	<input type="radio"/> Local <input checked="" type="radio"/> SNTP
Date	01/01/1970 (MM/DD/YYYY)
Time	00:02:40 (HH:MM:SS)
Time Zone Name	
Offset Hours	8 (-2 to 13)
Offset Minutes	0 (0 to 59)
Time Zone Reference	

SKS7300-12GPY2XGT2XGS

System Switching QoS Security Monitoring Maintenance English Save Logout

Management Deviceview Services DNS SNMP LLDP ISDP Timer Schedule

**Management**

- System Information
- Hardware Information
- Device Information
- Switch Statistics
- System CPU Status
- Network Interface
- Time
- Time Configuration
- SNTP Global Configuration**
- SNTP Server Configuration
- DayLight Saving Configuration

SNTP Global Configuration - Configuration

Apply Refresh

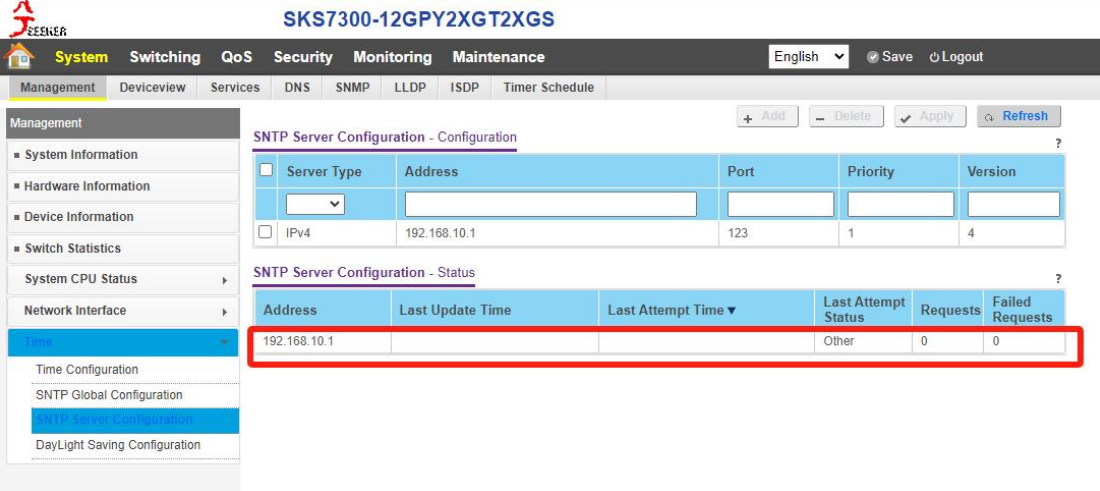
Client Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Unicast <input type="radio"/> Broadcast
Port	123 (123, 1025 to 65535)
Source Interface	None
Unicast Poll Interval	6 (6 to 10) power of two seconds, e.g. 10 -> 1024 seconds, 6 -> 64 seconds
Broadcast Poll Interval	6 (6 to 10) power of two seconds, e.g. 10 -> 1024 seconds, 6 -> 64 seconds
Unicast Poll Timeout	5 (1 to 30) seconds, e.g. 10 -> 10 seconds
Unicast Poll Retry	3 (0 to 10)

SNTP Global Configuration - Status

Version	4
Supported Mode	
Last Update Time	Not Synchronized
Last Attempt Time	
Last Attempt Status	Other
Server IP Address	
Address Type	unknown
Server Stratum	0
Reference Clock Id	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	0
Broadcast Count	0

If SNTP is working properly, the default is to send a query message once every 64s, that is, every 64s, it will confirm the connectivity with the server.

After working properly, the chart below will show the number of queries, last update time, and other information.



SKS7300-12GPY2XGT2XGS

System Switching QoS Security Monitoring Maintenance English Save Logout

Management Deviceview Services DNS SNMP LLDP ISDP Timer Schedule

Management

- System Information
- Hardware Information
- Device Information
- Switch Statistics
- System CPU Status
- Network Interface
- Time
- Time Configuration
- SNTP Global Configuration
- SNTP Server Configuration
- DayLight Saving Configuration

SNTP Server Configuration - Configuration

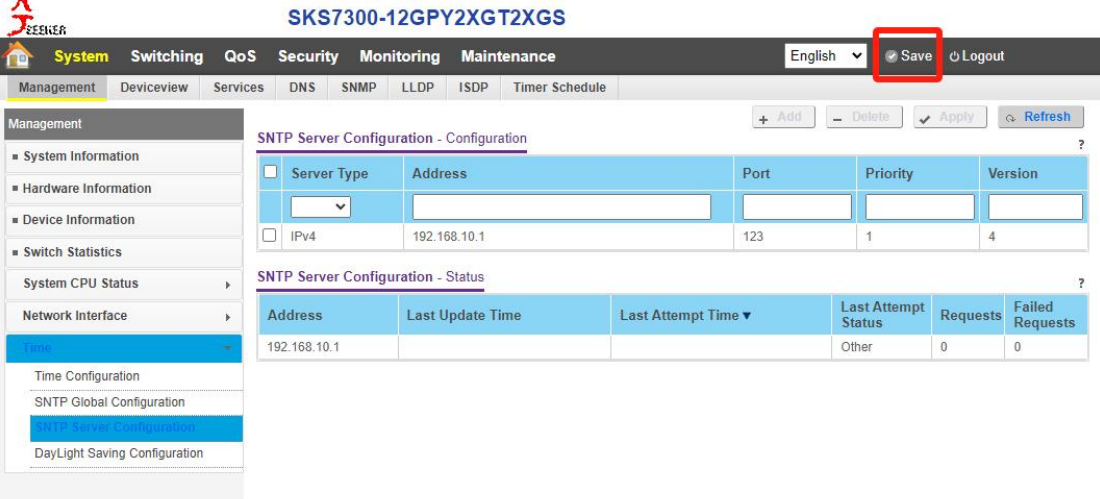
Server Type	Address	Port	Priority	Version
<input type="checkbox"/> IPv4	192.168.10.1	123	1	4

SNTP Server Configuration - Status

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
192.168.10.1			Other	0	0

#### (5) Save Settings

At the top right of the interface there is a save button, which can be used at any time to save the configuration by clicking on the save button.



SKS7300-12GPY2XGT2XGS

System Switching QoS Security Monitoring Maintenance English Save Logout

Management Deviceview Services DNS SNMP LLDP ISDP Timer Schedule

Management

- System Information
- Hardware Information
- Device Information
- Switch Statistics
- System CPU Status
- Network Interface
- Time
- Time Configuration
- SNTP Global Configuration
- SNTP Server Configuration
- DayLight Saving Configuration

SNTP Server Configuration - Configuration

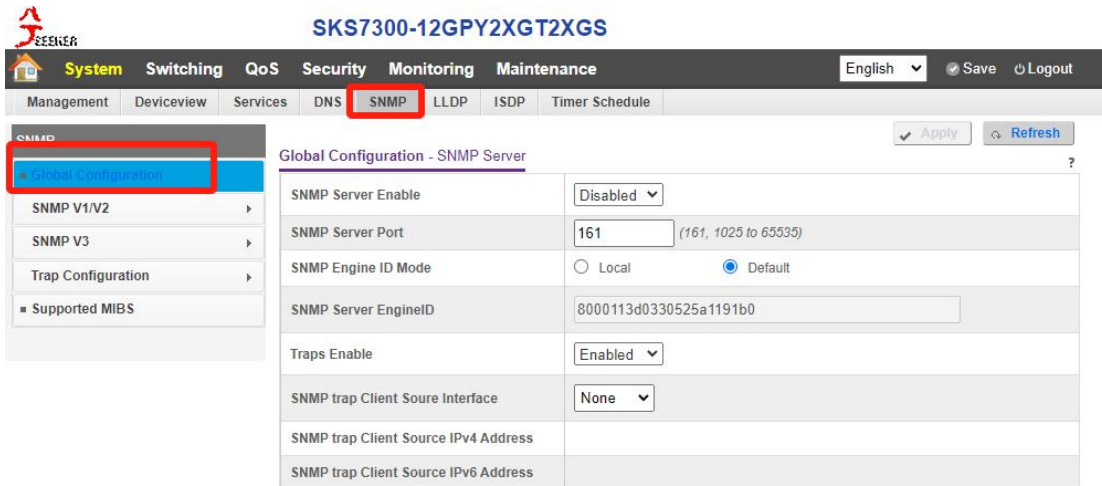
Server Type	Address	Port	Priority	Version
<input type="checkbox"/> IPv4	192.168.10.1	123	1	4

SNTP Server Configuration - Status

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
192.168.10.1			Other	0	0

#### (6) SNMP Management

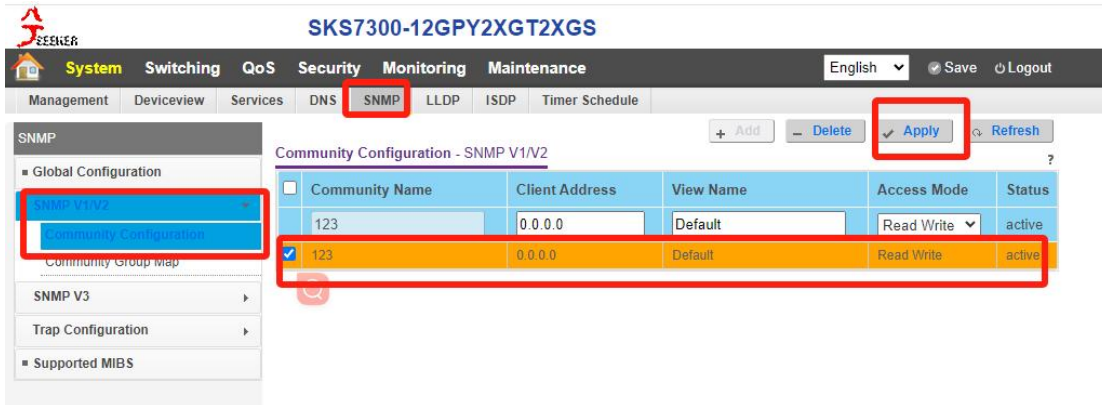
In System Management-SNMP Management, you can configure SNMP related information. First you need to turn on the SNMP server working mode, then you can set the SNMP port number.



Global Configuration - SNMP Server

SNMP Server Enable	Disabled
SNMP Server Port	161 (161, 1025 to 65535)
SNMP Engine ID Mode	Local <input type="radio"/> Default <input checked="" type="radio"/>
SNMP Server EngineID	8000113d0330525a1191b0
Traps Enable	Enabled
SNMP trap Client Source Interface	None
SNMP trap Client Source IPv4 Address	
SNMP trap Client Source IPv6 Address	

In SNMPv1/v2, configure the community name, client address, view name, and access mode, and after configuring them, select Add in the upper-right corner and click Apply.



Community Configuration - SNMP V1/V2

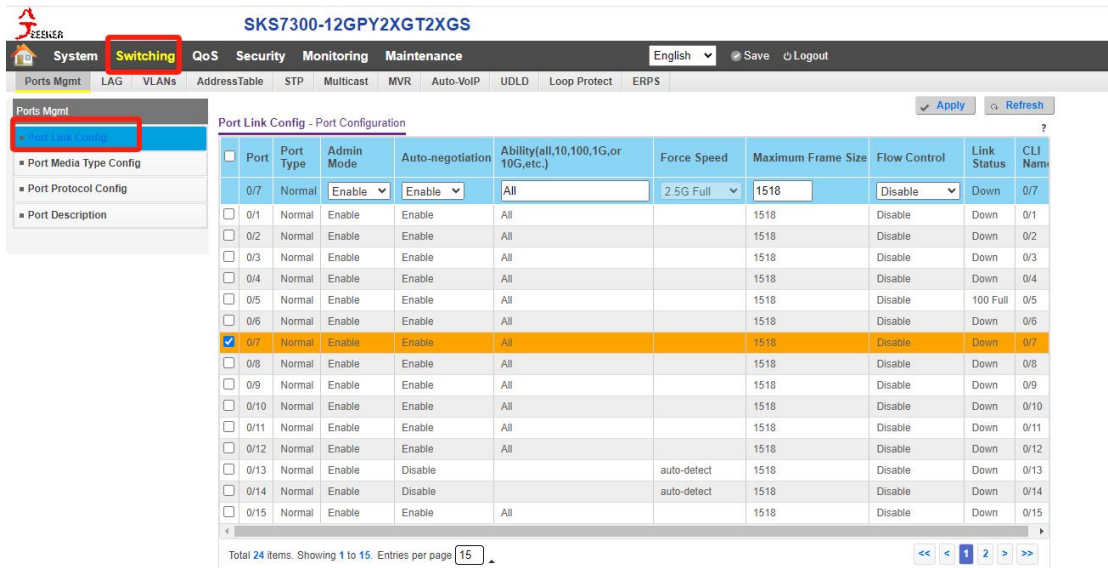
<input type="checkbox"/>	Community Name	Client Address	View Name	Access Mode	Status
<input type="checkbox"/>	123	0.0.0.0	Default	Read Write	active
<input checked="" type="checkbox"/>	123	0.0.0.0	Default	Read Write	active

## 3.L2 Switching Management

### (7) Port Management

The port management interface can be turned off to enable the port, you can turn off or turn on the port adaptive mode, turn on the port by default is the auto-negotiated rate, turn off to force the port rate.

**Note:** It is not recommended to force the rate of the electrical port, it may cause the switch to become unusable, just keep auto-negotiation.

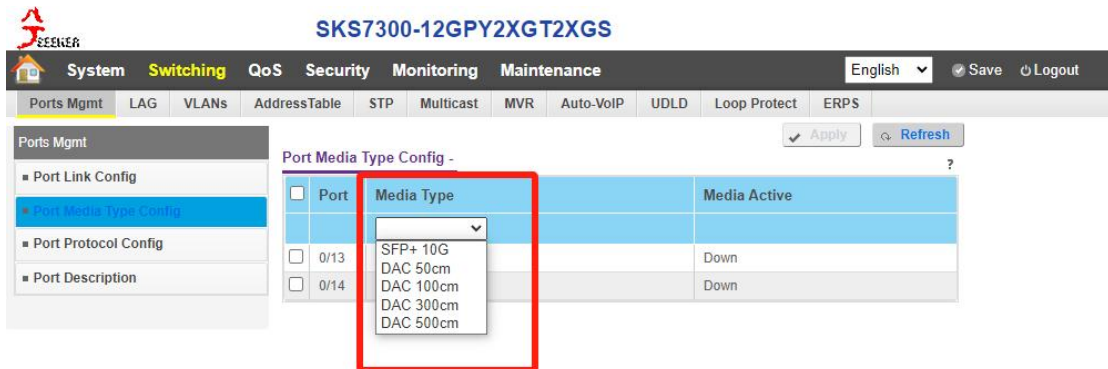


Port	Port Type	Admin Mode	Auto-negotiation	Ability(all,10,100,1G,or 10G,etc.)	Force Speed	Maximum Frame Size	Flow Control	Link Status	CLI Name
<input type="checkbox"/> 0/1	Normal	Enable	Enable	All		1518	Disable	Down	0/1
<input type="checkbox"/> 0/2	Normal	Enable	Enable	All		1518	Disable	Down	0/2
<input type="checkbox"/> 0/3	Normal	Enable	Enable	All		1518	Disable	Down	0/3
<input type="checkbox"/> 0/4	Normal	Enable	Enable	All		1518	Disable	Down	0/4
<input type="checkbox"/> 0/5	Normal	Enable	Enable	All		1518	Disable	100 Full	0/5
<input type="checkbox"/> 0/6	Normal	Enable	Enable	All		1518	Disable	Down	0/6
<input checked="" type="checkbox"/> 0/7	Normal	Enable	Enable	All	2.5G Full	1518	Disable	Down	0/7
<input type="checkbox"/> 0/8	Normal	Enable	Enable	All		1518	Disable	Down	0/8
<input type="checkbox"/> 0/9	Normal	Enable	Enable	All		1518	Disable	Down	0/9
<input type="checkbox"/> 0/10	Normal	Enable	Enable	All		1518	Disable	Down	0/10
<input type="checkbox"/> 0/11	Normal	Enable	Enable	All		1518	Disable	Down	0/11
<input type="checkbox"/> 0/12	Normal	Enable	Enable	All		1518	Disable	Down	0/12
<input type="checkbox"/> 0/13	Normal	Enable	Disable		auto-detect	1518	Disable	Down	0/13
<input type="checkbox"/> 0/14	Normal	Enable	Disable		auto-detect	1518	Disable	Down	0/14
<input type="checkbox"/> 0/15	Normal	Enable	Enable	All		1518	Disable	Down	0/15

Jumbo frames (maximum frame length) as well as flow control can also be set in the port management interface. You can look at the last two columns to see the connection status of the port and the name in the CLI command line.

For optical ports, you do not need to force the rate when connecting to 10G devices, and you need to force the port to the corresponding rate when connecting to 2.5G or 1G devices.

When using DAC or AOC cables, in the Port Media Type Config, you can select the DAC option corresponding to the length of the media category (AOC also selects the corresponding DAC option).



Port	Media Type	Media Active
<input type="checkbox"/> 0/13	SFP+ 10G DAC 50cm DAC 100cm DAC 300cm DAC 500cm	Down
<input type="checkbox"/> 0/14		Down

## (8) Convergence Group Management

If you want to realize the link aggregation function of the intranet, you need to set it up in L2 Switching Management-Aggregation Group Management-Basic Management Information-Aggregation Members. The setting method is as follows:

First select the aggregation ID and then click on the port map below. a check mark will appear after clicking on the interface to indicate that the port has been added to this aggregation group.

**Note here: ports on the device that need to be aggregated together should be added to an**



aggregation group. Click Apply on the top right to apply the settings after you have made your selection.

If you want to set up static link aggregation, keep the default Enable for static mode.

If you want to set dynamic link aggregation, select Disable for static mode.

Step 1: Select the aggregation ID, choose any one, the aggregation name does not need to be changed

Step 2: Select the ports to be aggregated, such as port 11 and port 12

Step 3: Disable on behalf of dynamic convergence, generally in order to increase the speed of dynamic convergence should be selected,

Step 4: Apply first, then save

Note: No need to make any changes in other places.

About convergence after the transfer speed is not stable or not up to standard basically is the computer network card driver performance, jumbo frames, firewalls, hard disk speed, computer performance and so on a variety of factors lead to, for example, on the 2-disk NAS, that the speed of the speed is certainly not to run to 10,000 megabytes, the speed will not increase.

Additional topics to add, most of friends now have NAS storage, NAS for a higher connection speed is still very important, especially when more than one person at the same time to access the files in the NAS, the network traffic jam will greatly reduce the use of experience, this time we need link aggregation to solve the problem.

NAS generally provides a variety of link aggregation modes to choose from. Adaptive Load Balancing] mode is equivalent to the auto option, when the switch does not support the link aggregation function, we can choose this option, NAS will automatically help us to dual-port load balancing, to improve the speed of reading and writing when multiple users access at the same time; [IEEE802.3ad Dynamic Aggregation] and [Balance XOR] corresponds to the dynamic and static managed switches to support the 2 kinds of link aggregation modes, Ruoxi generally provides a variety of link aggregation modes to choose from. The [IEEE802.3ad Dynamic Aggregation] and [Balanced XOR] correspond to the dynamic and static modes supported by managed switches. Refer to the above tutorial for the switch setup tutorial.

#### (9) VLAN Management

The first step is to create VLANs.

In Switching - VLAN-Basic -VLAN Configuration.



Enter the VLAN number you need to add in VLANID, for example, if you need to add VLANID2, enter the number 2 in the first line, and then click Add in the upper-right corner to add VLANs. meanwhile, you can delete VLANs after checking the corresponding VLANs. click Apply after you have set up the VLANs.

The screenshot shows the XikeStor web interface for device SKS7300-12GPY2XGT2XGS. The 'Switching' menu is active, and the 'VLANs' sub-menu is selected. The interface includes a sidebar with 'VLAN' configuration options (Basic, Advanced, Protocol VLANs, 802.1Q TUNNELING, Voice VLAN Configuration) and a main content area with three configuration sections: 'VLAN Configuration - VLAN Reset', 'VLAN Configuration - Internal VLAN Configuration', and 'VLAN Configuration - VLAN Configuration'. The 'Add' button in the top right of the main area is highlighted with a red box. The 'VLAN Configuration - VLAN Configuration' section contains a table with columns for 'VLAN ID (likes: 2, 5-10)', 'VLAN Name(Max: 64 characters)', 'VLAN Type', and 'Make Static'. The first row of the table has '3' entered in the 'VLAN ID' field, which is also highlighted with a red box. The second row shows '1' in the 'VLAN ID' field and 'default' in the 'VLAN Name' field.

VLAN ID (likes: 2, 5-10)	VLAN Name(Max: 64 characters)	VLAN Type	Make Static
3			
1	default	Default	Disable

After creating VLANs, go to Advanced - Port PVID Configuration - here you can configure the port class and default VLAN ID, and the switch port modes are divided into general, access, and trunk. let's get straight to the practical work.

For example, if we want to classify port 2 into the newly created VLANID2 just now, we have to go to VLAN Management-Advanced Attribute Configuration-Port Attribute Configuration, check port 02, change the working mode to access, and then fill in the number 2 in the default VLAN of access, and click Apply to do it, so that port 2 is classified into VLAN2, and at this time, there is no communication between port 2 and all other ports. port 2 and all other ports cannot communicate with each other. If you want to set up more than one VLAN, the setting method is the same.

The screenshot displays the 'Port PVID Configuration - Access Mode' page in the XikeStor web interface. The navigation menu at the top includes 'System', 'Switching', 'QoS', 'Security', 'Monitoring', and 'Maintenance'. The 'VLANs' menu item is highlighted. The main content area shows a table of ports with the following columns: 'Interface', 'Switchport Mode', and 'Access Mode VLAN'. The table lists ports from 0/1 to 0/15, all currently set to 'General' mode and '1' for the Access Mode VLAN. Annotations in red text provide instructions: '1. Check the box first and select the port you want to set' (pointing to a checkbox), '2. To select the port mode, change to Access' (pointing to a dropdown menu), and '3. Enter the number 2 in the Access default VLAN' (pointing to a text input field).

The above is how to set up VLAN

The specific configuration tutorial for VLANs in dual broadband aggregation is as follows

As a reminder, the premise of broadband aggregation is that you must change the router dialup. This tutorial applies to pon sticks, the setup is the same.

We first assume that the scene is as follows, the setup steps are as follows: respectively, from the lan port of the two optical cats to connect the network cable to any port of the switch, such as the optical cat A to the switch's port 2, the optical cat B to the switch's port 3, and then the switch's port 4 to connect to the soft router WAN port, the router's lan port back to the switch's port 5 connects to a cable, the switch's remaining ports can be accessed on the Internet. Here we carry out the detailed configuration.

First of all, enter the port attribute configuration interface of the switch, set port 2 to VLANID2, refer to the above tutorial, and similarly configure port 3 to VLANID3. Then configure port 4 to VLANID4.

Then to the VLANTrunking mode configuration interface, because we go to port 4 to connect the soft routing, so port 4 should be set to trunk mode can be, while the default VLANID should be filled in the 4 can be, and then allow VLAN2 and VLAN3 through the trunk port to access the router, the specific device approach to refer to the picture in the steps.

SKS7300-12GPY2XGT2XGS

System **Switching** QoS Security Monitoring Maintenance

Ports Mgmt LAG VLANs AddressTable STP Multicast MVR Auto-VoIP UDLD Loop Protect ERPS

VLAN

Basic

Advanced

VLAN Configuration

Port PVID Configuration

Port VLAN Configuration

Port VLAN Membership

Port Default Priority

VLAN Status

Port VLAN Status

GARP Switch Configuration

GARP Port Configuration

Protocol VLANs

802.1Q TUNNELING

Voice VLAN Configuration

1. Check port 04

2. Change the working mode to trunk

3. Change the default VLAN ID to 4.

4. set port 4 to allow the passage of VLAN 2 and 3 fill in, of course, if you are three broadband, you can also fill in 2,3,6

VLAN Trunking Configuration - Trunk Mode

Interface	Switchport Mode	Native VLAN ID	Trunk Allowed VLANs	Trunk Except VLANs
<input type="checkbox"/> 0/1	General	1	All	
<input type="checkbox"/> 0/2	General	1	All	
<input type="checkbox"/> 0/3	General	1	All	
<input type="checkbox"/> 0/4	General	1	All	
<input type="checkbox"/> 0/5	General	1	All	
<input type="checkbox"/> 0/6	General	1	All	
<input type="checkbox"/> 0/7	General	1	All	
<input type="checkbox"/> 0/8	General	1	All	
<input type="checkbox"/> 0/9	General	1	All	
<input type="checkbox"/> 0/10	General	1	All	
<input type="checkbox"/> 0/11	General	1	All	
<input type="checkbox"/> 0/12	General	1	All	
<input type="checkbox"/> 0/13	General	1	All	
<input type="checkbox"/> 0/14	General	1	All	
<input type="checkbox"/> 0/15	General	1	All	

Total 24 items. Showing 1 to 15. Entries per page 15

Final step: connect a cable from the router lan port to any remaining port of the switch, and you can access the internet normally!

Of course, this is just an example, you can connect to port 8 port 9 or any other port, if you have more than 2 broadband need to converge, the method is the same, please read and write the tutorial can be realized. As for how much broadband aggregation can improve the speed, there is no way to predict, because there are many factors affecting.

## (10) MAC Management

You can view all the MAC addresses learned by each port of the switch in Switching - AddressTable - Basic - Address Table - MAC Status, and a port can learn multiple MAC addresses. In AddressTable - Advanced, you can

(1) Configure the dynamic MAC address aging time, the default is 300s.

(2) Configure static MAC address, that is, configure static table entries in the switch's MAC address table

SKS7300-12GPY2XGT2XGS

System **Switching** QoS Security Monitoring Maintenance

Ports Mgmt LAG VLANs **AddressTable** STP Multicast MVR Auto-VoIP UDLD Loop Protect ERPS

AddressTable

Basic

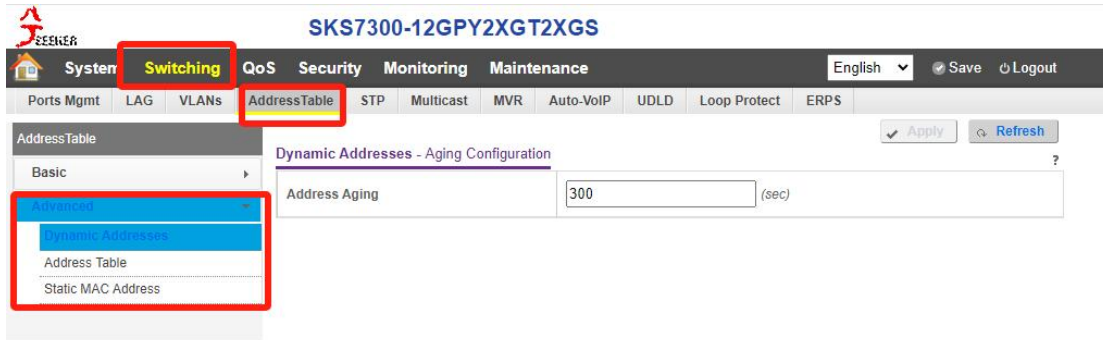
Advanced

Address Table - MAC Status

Total MAC Addresses: 2

Search By VLAN ID Search

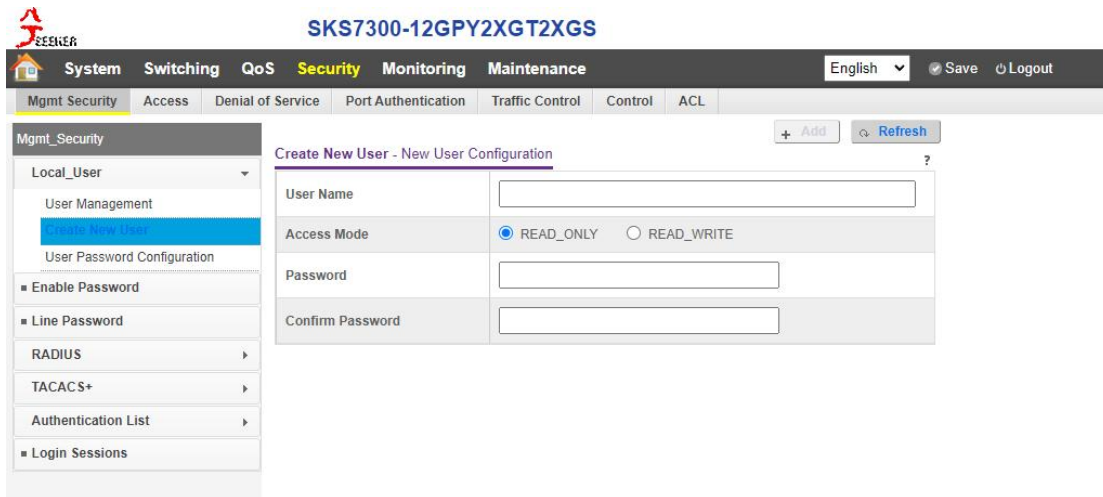
VLAN ID	MAC Address	Interface	Status
1	00:E0:4C:68:B4:39	0/5	Learned
1	30:52:5A:11:91:B0	cpu	Management



The screenshot shows the XikeStor web interface for device SKS7300-12GPY2XGT2XGS. The navigation menu includes System, Switching, QoS, Security, Monitoring, and Maintenance. Under Switching, the AddressTable sub-menu is expanded, showing options for Basic, Advanced, Dynamic Addresses, Address Table, and Static MAC Address. The main content area displays the 'Dynamic Addresses - Aging Configuration' page, where the 'Address Aging' field is set to 300 seconds.

## 4. Security Management

### (11) Add New User

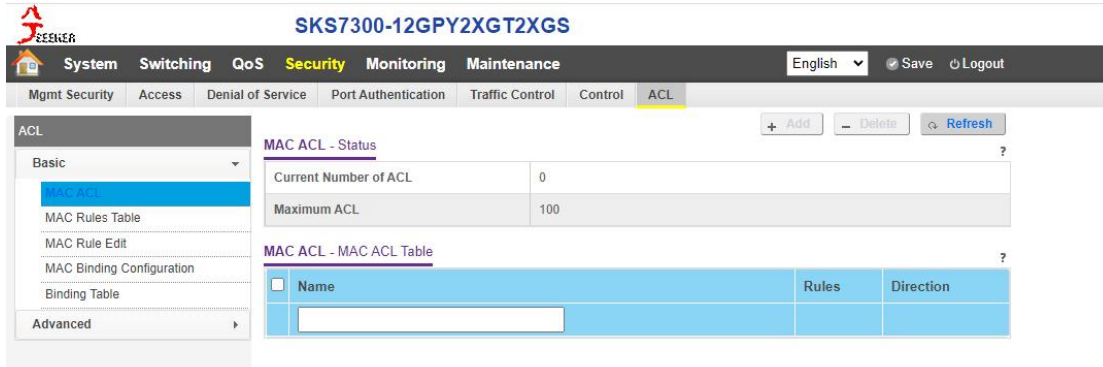


The screenshot shows the XikeStor web interface for device SKS7300-12GPY2XGT2XGS. The navigation menu includes System, Switching, QoS, Security, Monitoring, and Maintenance. Under Security, the Mgmt\_Security sub-menu is expanded, showing options for Local\_User, User Management, Create New User, and User Password Configuration. The 'Create New User' sub-menu is highlighted in blue. The main content area displays the 'Create New User - New User Configuration' page, which includes fields for User Name, Access Mode (with READ\_ONLY selected), Password, and Confirm Password.

In Security - Mgmt\_Security - Local\_Users - Create New User, enter the user name and password, and select the access mode. After setting, select +Add in the upper right corner to add users.

### (12) Setting the ACL

In Security - ACL, you can set ACLs, and the system supports setting Layer 2 ACLs and Layer 3 ACLs.



SKS7300-12GPY2XGT2XGS

System Switching QoS **Security** Monitoring Maintenance English Save Logout

Mgmt Security Access Denial of Service Port Authentication Traffic Control Control **ACL**

ACL

Basic

MAC ACL

MAC Rules Table

MAC Rule Edit

MAC Binding Configuration

Binding Table

Advanced

MAC ACL - Status

Current Number of ACL 0

Maximum ACL 100

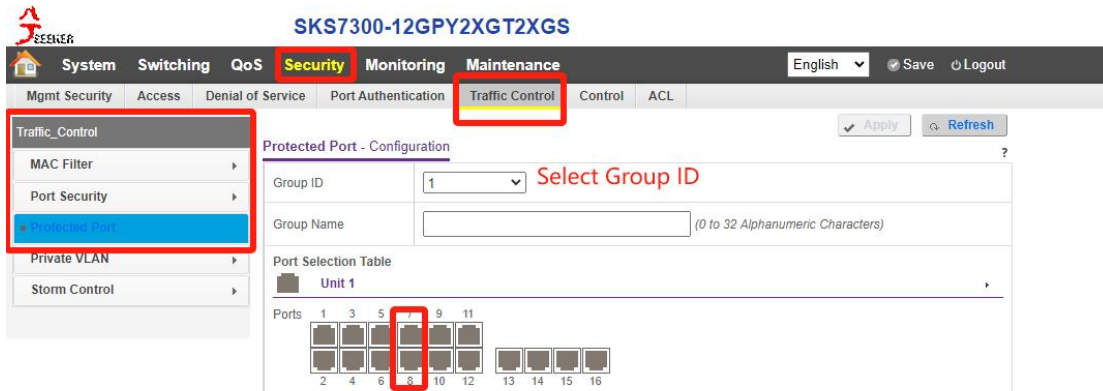
MAC ACL - MAC ACL Table

Name	Rules	Direction

### (13) Port Isolation

In Security - Traffic Control - Protected Port.

Select the group ID for isolation (up to 3 isolation groups are supported), and then check the ports to be isolated below. Ports in the same isolation group cannot communicate, and ports in different isolation groups can communicate.



SKS7300-12GPY2XGT2XGS

System Switching QoS **Security** Monitoring Maintenance English Save Logout

Mgmt Security Access Denial of Service Port Authentication **Traffic Control** Control ACL

Traffic\_Control

MAC Filter

Port Security

**Protected Port**

Private VLAN

Storm Control

Protected Port - Configuration

Group ID 1 Select Group ID

Group Name (0 to 32 Alphanumeric Characters)

Port Selection Table

Unit 1

Ports

1	3	5	7	9	11
2	4	6	8	10	12

Check the port for isolation, ports in the same isolation group cannot communicate

## 5. Monitoring Management

### (14) Port Information

You can see port statistics, port traffic collection information, and port link status in the Monitoring - Ports

### (15) Mirror Management

In Monitoring - Mirroring you can configure the source port, destination port and direction of the mirror packet.



Select sessionID in Mirroring Configuration, up to 4 sessionIDs can be created, and then select Enable in Working Mode to turn on the port mirroring group.

Then select the destination port as the monitoring port, you can select the mirroring port in the table below, just check the corresponding port, then select the direction of the mirrored packet text, click Apply in the upper right corner after you have made your selection.

The mirroring configuration of the first item on the left is only switch local mirroring, that is to say, both the mirroring port and the observation port are on the same switch, if you need to be on a different switch, you need to configure RSPAN.

SKS7300-12GPY2XGT2XGS

System Switching QoS Security **Monitoring** Maintenance English Save Logout

Ports **Mirroring** sFlow Log

Mirroring

- Port Mirroring
- RSPAN VLAN
- RSPAN Source Switch Configuration
- RSPAN Destination Switch Configuration

Port Mirroring - Global Configuration

Session ID: 1

Admin Mode:  Disable  Enable

Destination Interface: None

Filter Type: None

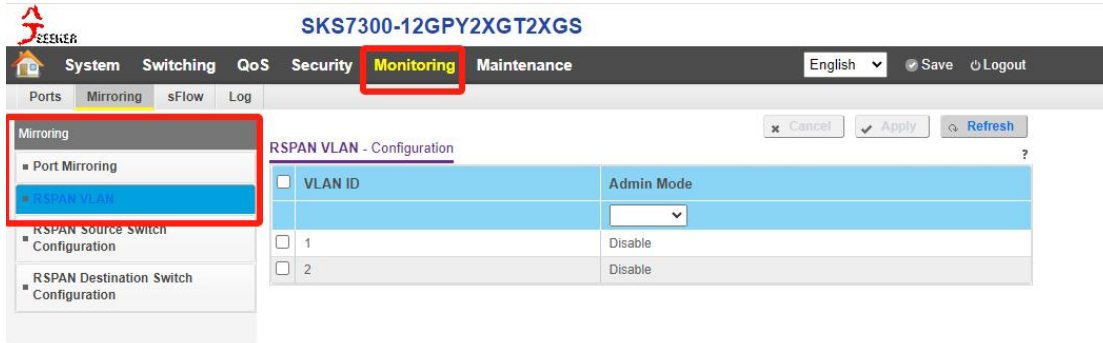
Filter Name:

Port Mirroring - Source Interface Configuration

Source Port	Direction	Status
<input type="checkbox"/>	None	
<input type="checkbox"/> 0/1	None	
<input type="checkbox"/> 0/2	None	
<input type="checkbox"/> 0/3	None	
<input type="checkbox"/> 0/4	None	
<input type="checkbox"/> 0/5	None	
<input type="checkbox"/> 0/6	None	
<input type="checkbox"/> 0/7	None	
<input type="checkbox"/> 0/8	None	
<input type="checkbox"/> 0/9	None	
<input type="checkbox"/> 0/10	None	
<input type="checkbox"/> 0/11	None	
<input type="checkbox"/> 0/12	None	
<input type="checkbox"/> 0/13	None	
<input type="checkbox"/> 0/14	None	
<input type="checkbox"/> 0/15	None	

Total 26 items. Showing 1 to 15. Entries per page 15

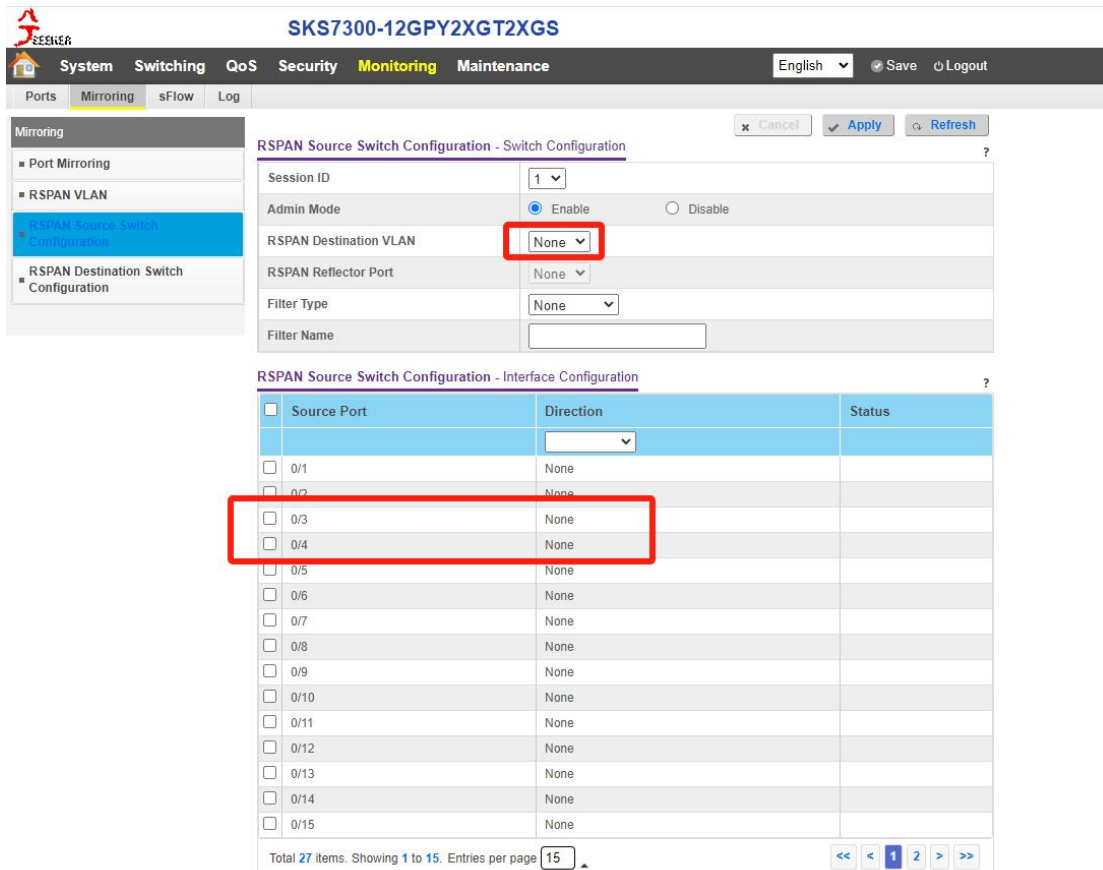
Then we describe how to configure Layer 2 remote port mirroring, or RSPAN. First set the VLAN to which the mirrored traffic belongs.



The screenshot shows the XikeStor web interface for device SKS7300-12GPY2XGT2XGS. The 'Monitoring' tab is selected. In the left sidebar, 'RSPAN VLAN' is highlighted. The main area shows the 'RSPAN VLAN - Configuration' table:

VLAN ID	Admin Mode
<input type="checkbox"/> 1	Disable
<input type="checkbox"/> 2	Disable

Then configure the source switch, first selecting the sessionID.  
 Select the VLAN to which the mirrored traffic just set belongs.  
 Check the source port of the mirrored traffic, select the direction of the mirrored message, and set the rest as needed.



The screenshot shows the 'RSPAN Source Switch Configuration - Switch Configuration' page. The 'RSPAN Source Switch Configuration' section is expanded, showing the following fields:

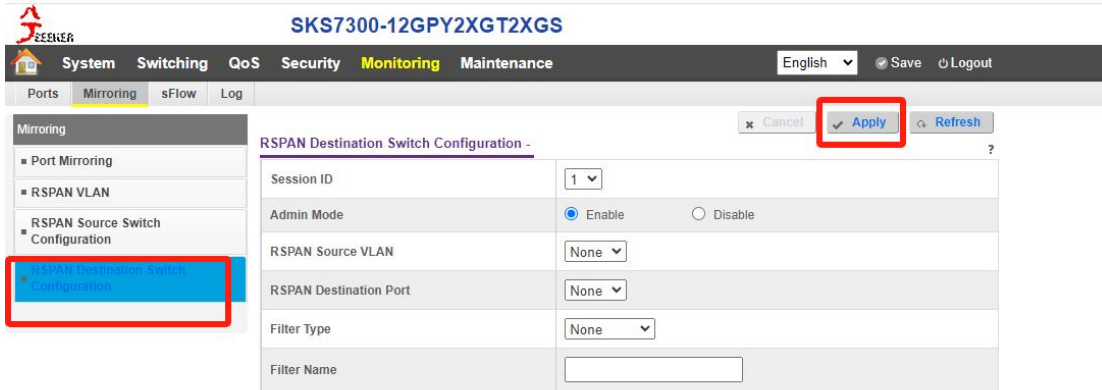
- Session ID: 1
- Admin Mode:  Enable
- RSPAN Destination VLAN: **None** (highlighted with a red box)
- RSPAN Reflector Port: None
- Filter Type: None
- Filter Name: (empty)

Below this is the 'RSPAN Source Switch Configuration - Interface Configuration' table:

Source Port	Direction	Status
<input type="checkbox"/> 0/1	None	
<input type="checkbox"/> 0/2	None	
<input type="checkbox"/> 0/3	None	
<input type="checkbox"/> 0/4	None	
<input type="checkbox"/> 0/5	None	
<input type="checkbox"/> 0/6	None	
<input type="checkbox"/> 0/7	None	
<input type="checkbox"/> 0/8	None	
<input type="checkbox"/> 0/9	None	
<input type="checkbox"/> 0/10	None	
<input type="checkbox"/> 0/11	None	
<input type="checkbox"/> 0/12	None	
<input type="checkbox"/> 0/13	None	
<input type="checkbox"/> 0/14	None	
<input type="checkbox"/> 0/15	None	

The row for port 0/3 is highlighted with a red box. The bottom of the page shows 'Total 27 items. Showing 1 to 15. Entries per page 15'.

Then configure the destination switch. Select the sessionID you just set.  
 RSPAN source VLAN or select the VLAN to which the mirrored traffic belongs.  
 Then select the observation port of the destination switch. After you have configured it, click Apply.



SKS7300-12GPY2XGT2XGS

System Switching QoS Security **Monitoring** Maintenance English Save Logout

Ports Mirroring sFlow Log

Mirroring

- Port Mirroring
- RSPAN VLAN
- RSPAN Source Switch Configuration
- RSPAN Destination Switch Configuration**

RSPAN Destination Switch Configuration -

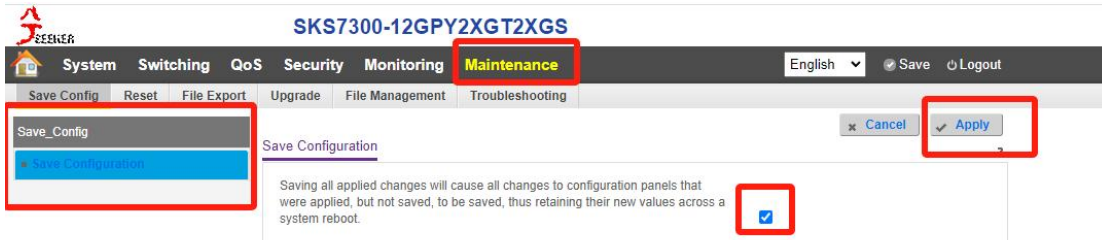
Cancel Apply Refresh

Session ID	1
Admin Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RSPAN Source VLAN	None
RSPAN Destination Port	None
Filter Type	None
Filter Name	

## 6.Maintenance

(16) Save Settings

Check the box in Maintenance - Save Configuration and click Apply to save the configuration.



SKS7300-12GPY2XGT2XGS

System Switching QoS Security Monitoring **Maintenance** English Save Logout

Save Config Reset File Export Upgrade File Management Troubleshooting

Save\_Config

- Save Configuration**

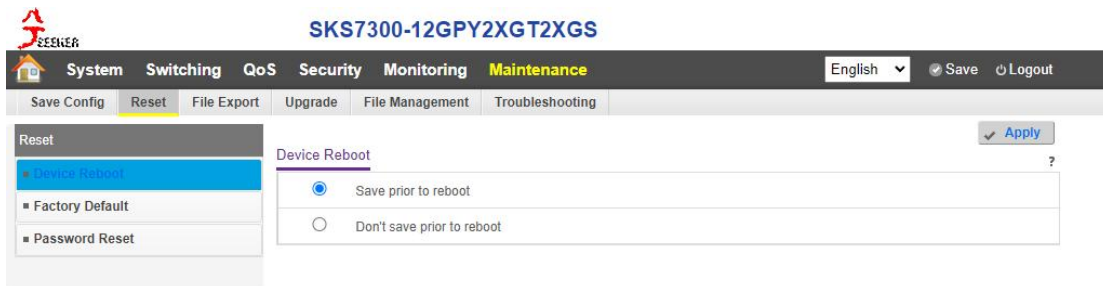
Save Configuration

Cancel Apply

Saving all applied changes will cause all changes to configuration panels that were applied, but not saved, to be saved, thus retaining their new values across a system reboot.

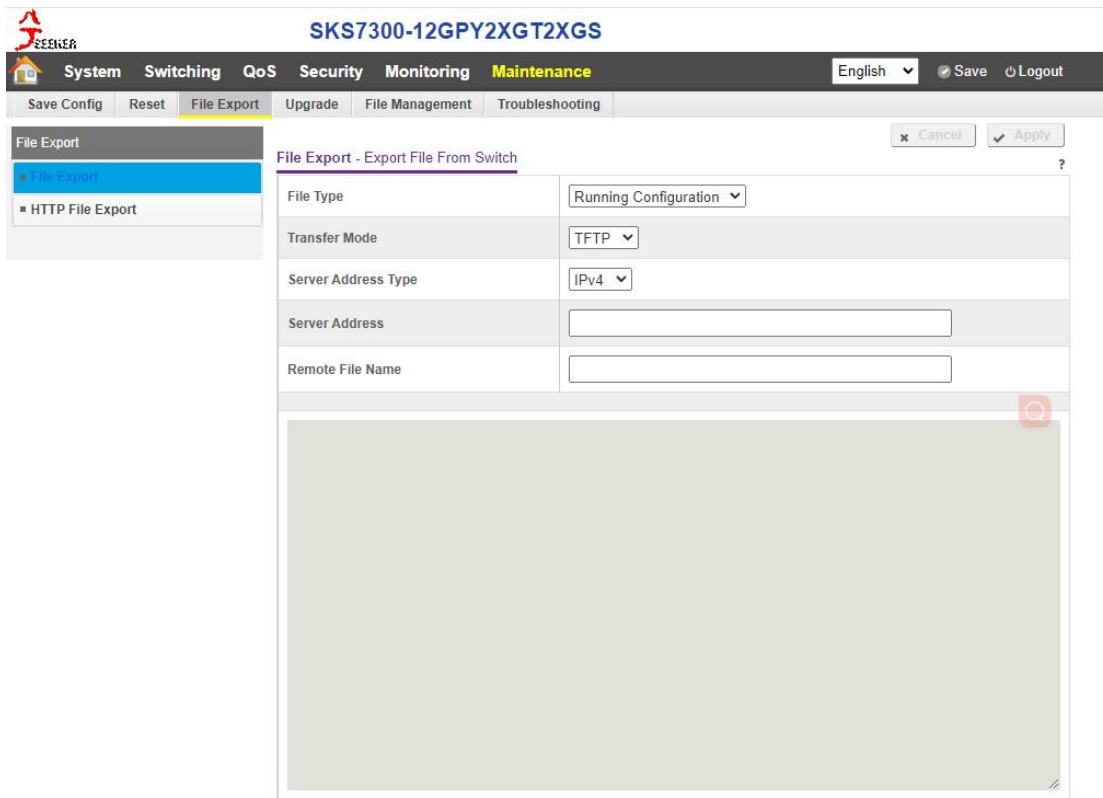
(17) Reboot

In Maintenance - Reset you can select Reboot Operation, Restore Factory Settings and Password Clear.



### (18) Download Configuration File

In Maintenance - File Export, you can select different file transfer protocols to download files from the switch, including FTP, SFTP, TFTP, SCP, and HTTP transfer protocols, and files including running configuration files, initial configuration files, error logs, and other files.



### (19) Updating Device Files

In Maintenance - Upgrade, you can upload a file and save it to the switch to update the switch configuration file.

SEEKER SKS7300-12GPY2XGT2XGS

System Switching QoS Security Monitoring **Maintenance** English Save Logout

Save Config Reset File Export Upgrade File Management Troubleshooting

Upgrade

- File Upgrade
- HTTP File Upgrade

File Upgrade - Import File to Switch

Cancel Apply

File Type	Startup Configuration
Transfer Mode	TFTP
Server Address Type	IPv4
Server Address	
Remote File Name	

## (20) IMG Document Management

In Maintenance - File Management, you can select and manage IMG firmware.

SEEKER SKS7300-12GPY2XGT2XGS

System Switching QoS Security Monitoring **Maintenance** English Save Logout

Save Config Reset File Export Upgrade File Management Troubleshooting

Filemanagement

- Copy
- Dual Image Configuration

Copy

Source Image	<input checked="" type="radio"/> Image1	<input type="radio"/> Image2
Destination Image	<input type="radio"/> Image1	<input checked="" type="radio"/> Image2

Apply Clear

## (21) Diagnostic Tool

In the Maintenance - Troubleshooting, you can perform ping tests to check connectivity, including both ipv4 and ipv6 ping tests.



- Troubleshooting
  - Ping IPv4
  - Ping IPv6**

Ping IPv6 - ?

Ping	Global
IPv6 Address	<input type="text"/> <small>(xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx. Max 255 characters)</small>
Count	3 <small>(1 to 15)</small>
Interval(secs)	1 <small>(1 to 60)</small>
Datagram Size	0 <small>(0 to 13000)</small>
Source	None
Ping Results:	

Apply Clear