XikeStor

ETHERNET SWITCH

WEB User Manual

Applicable Models

SKS3200-5E2X

SKS3200-5E2X-P

SKS3200-8E2X

SKS3200-8E2X-P

Document Version: V2.0
Language: English

Document Information

Item	Description
Product	XikeStor Managed Ethernet Switch
Applicable Models	SKS3200-5E2X; SKS3200-5E2X-P; SKS3200-8E2X; SKS3200-8E2X-P
Document Version	V2.0
Language	English
Note	(1) The web interface screenshots below use the SKS3200-8E2X as an example. (2) PoE cannot be turned on or off separately; it is automatically configured by the device.

NOTE: The appearance and available fields of the WEB interface may vary slightly with firmware revision. Use the interface displayed by the device as the reference.

1. System Functions

1.1 Log In to the Switch

Before logging in, configure the management PC with an IPv4 address in the same subnet as the switch. For the first login, use 192.168.10.x (x = 2 to 254) with subnet mask 255.255.255.0. Do not assign 192.168.10.12 to the PC because this is the default management address of the switch.

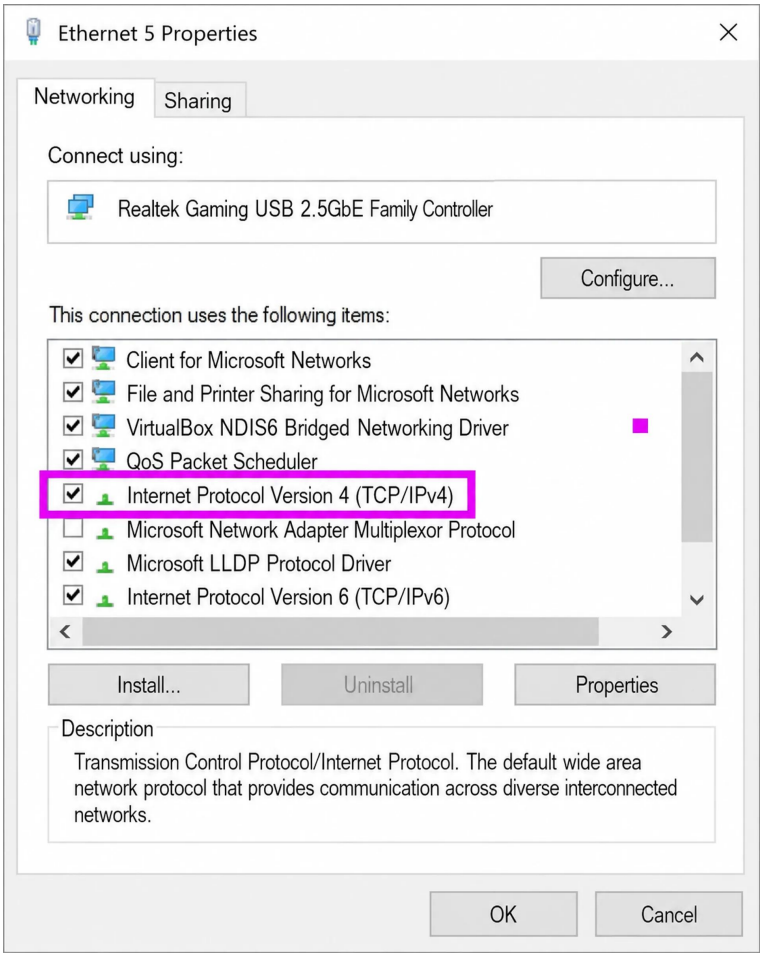

Figure 1-1. Configure the Management PC IP Address

Configure the PC network adapter with a static IPv4 address in the 192.168.10.0/24 subnet. The example shows the Windows IPv4 properties page.

NOTE: The PC must be physically connected to an Ethernet port on the switch before the WEB management page can be accessed.

Open a web browser and enter the switch management address. At the login page, enter the default user name admin and password admin, then select the login button to open the System Information page.

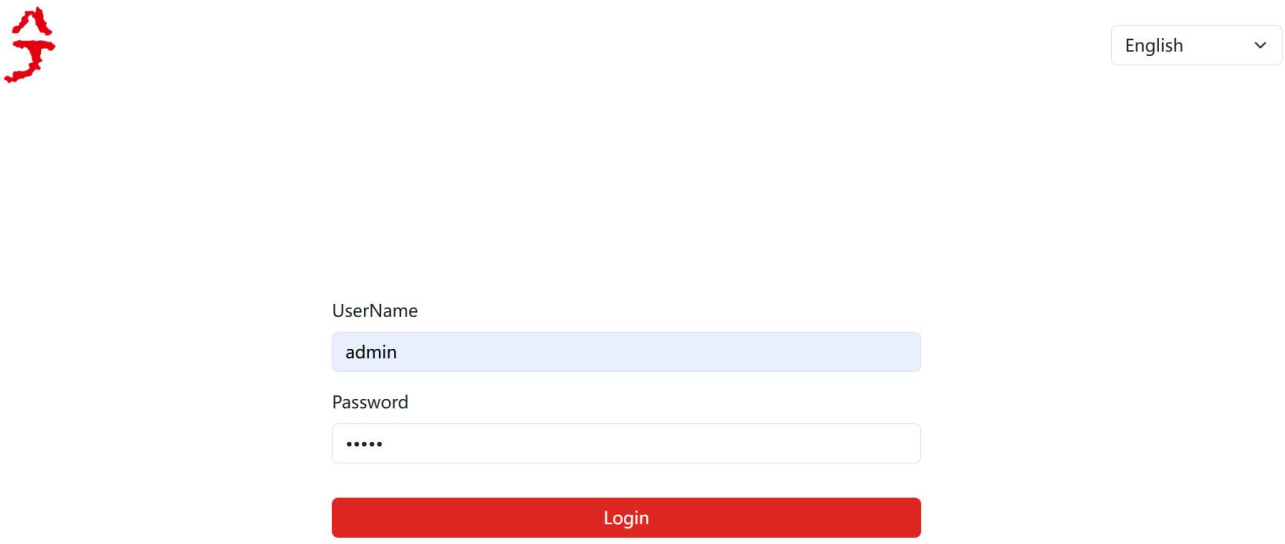

Figure 1-2. WEB Login Page

Enter the default credentials (admin/admin) to access the switch WEB management interface. Change the default password after the first login.

1.2 System Information

1. Select System Functions > System Information.
2. View or edit the device description and review the IPv4 address, IPv6 address, MAC address, firmware version, and other device information.

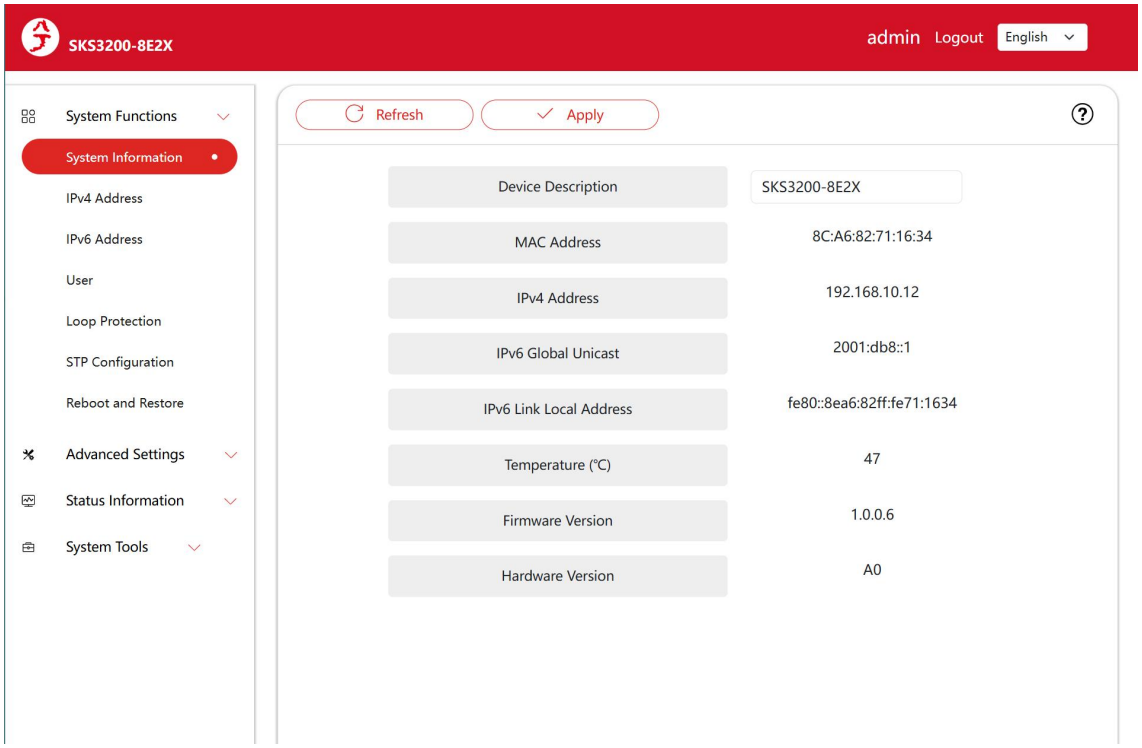

Figure 1-3. System Information

This page provides an overview of the switch identity, management addresses, hardware information, and installed firmware version.

1.3 IPv4 Address

3. Select System Functions > IPv4 Address.
4. Configure the IPv4 address used to access the switch management interface.

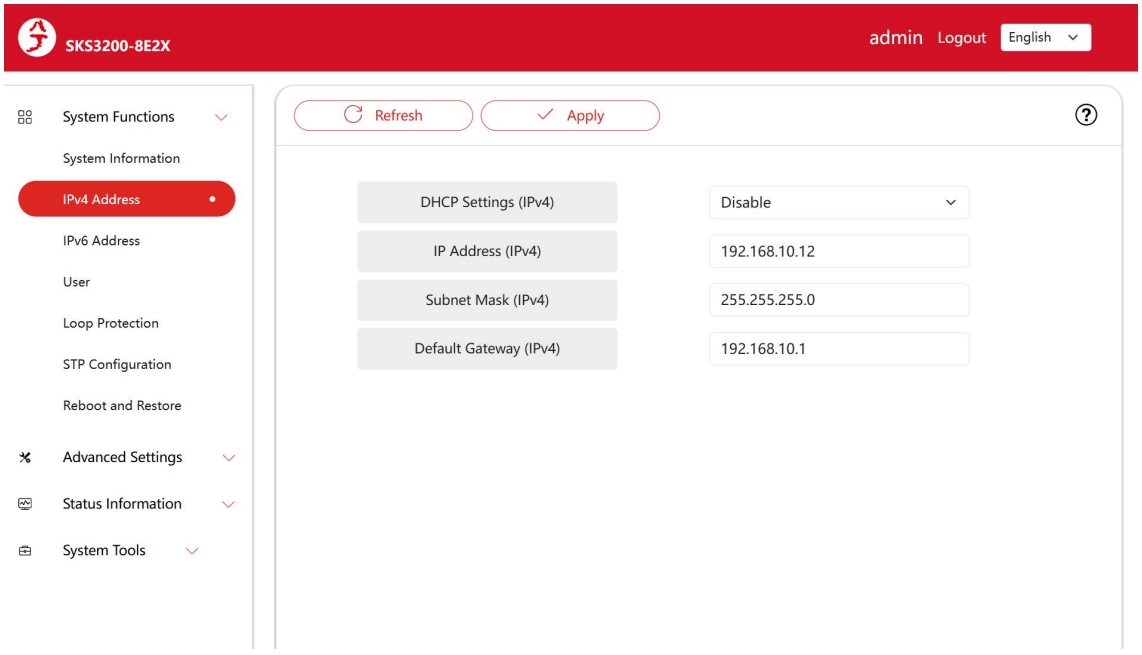

Figure 1-4. IPv4 Address Settings

Select static addressing or DHCP, then configure the management IP address, subnet mask, and default gateway as required.

Item	Description
DHCP Setting (IPv4)	Disabled: use a static IPv4 address. Enabled: obtain an IPv4 address automatically from a DHCP server.
IP Address (IPv4)	Management IPv4 address of the switch.
Subnet Mask (IPv4)	Subnet mask for the management IPv4 address.
Default Gateway (IPv4)	Default IPv4 gateway used by the switch.

1.4 User Management

5. Select System Functions > User.
6. Configure the user name and password used to log in to the switch.

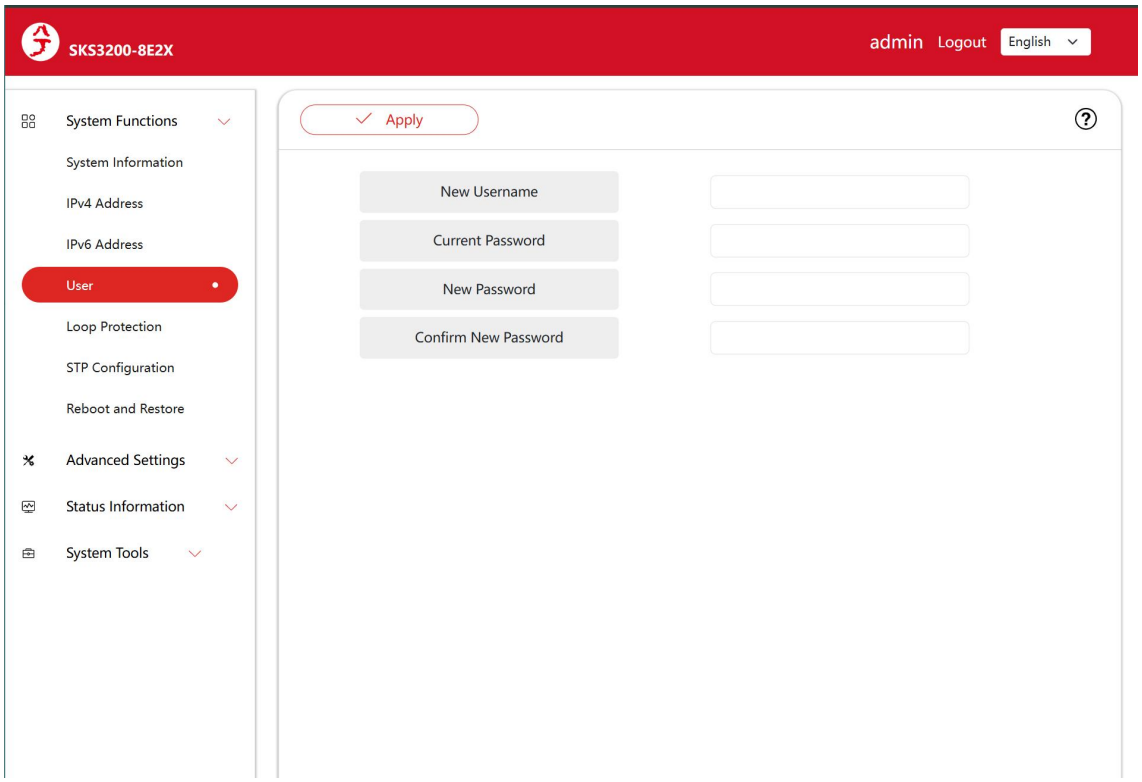

Figure 1-5. User Management

Use this page to update the WEB management login credentials. Store the new credentials securely.

1.5 Loop Protection and STP

7. Select System Functions > Loop and STP.
8. Configure loop protection and Spanning Tree Protocol (STP) functions for the switch.

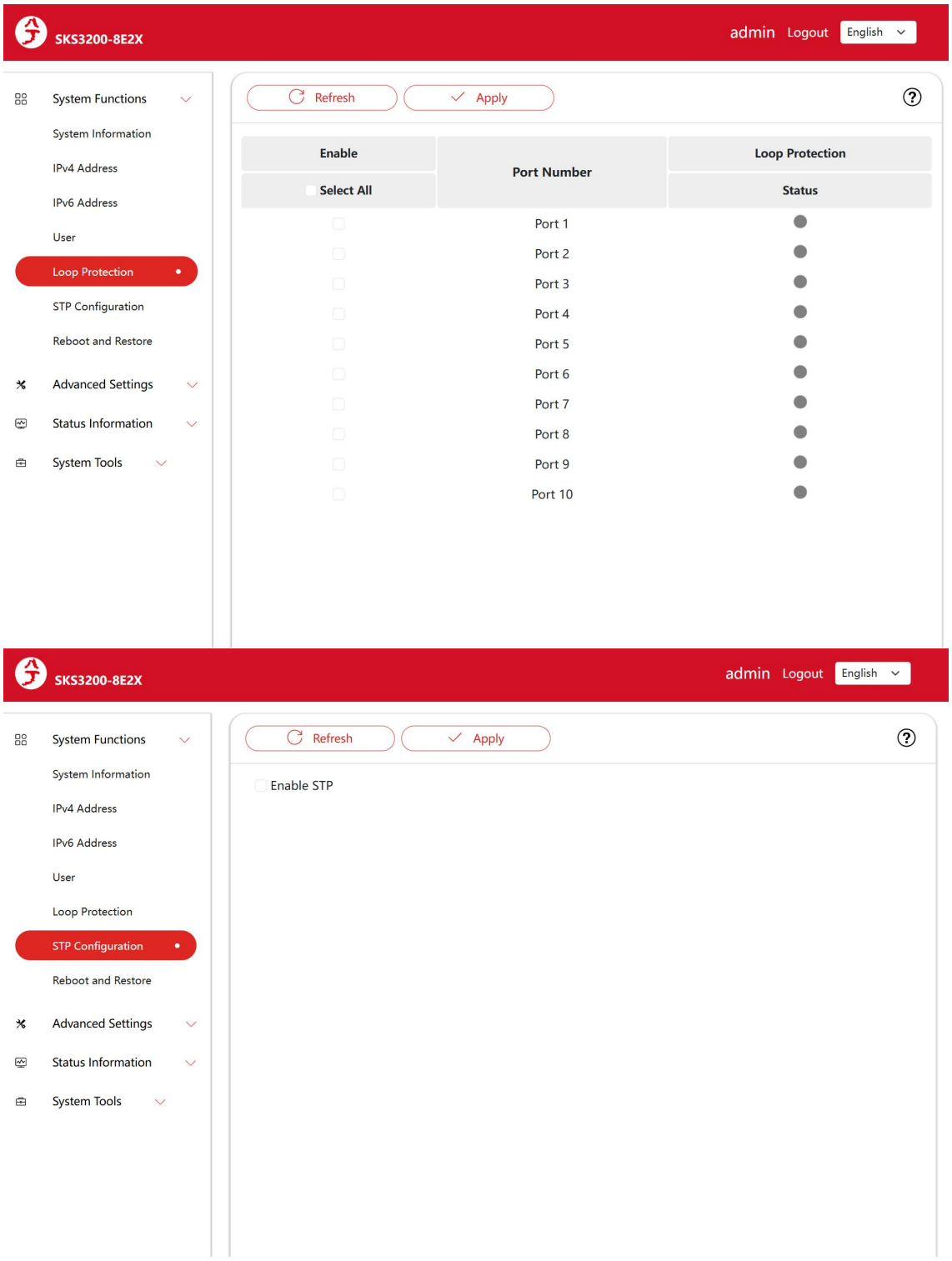

Figure 1-6. Loop Protection and STP

Enable the required loop prevention or STP functions and apply the settings according to the network topology.

1.6 Restart and Restore

9. Select System Functions > Restart and Restore.

10. Restart the switch or restore the device to its default configuration.

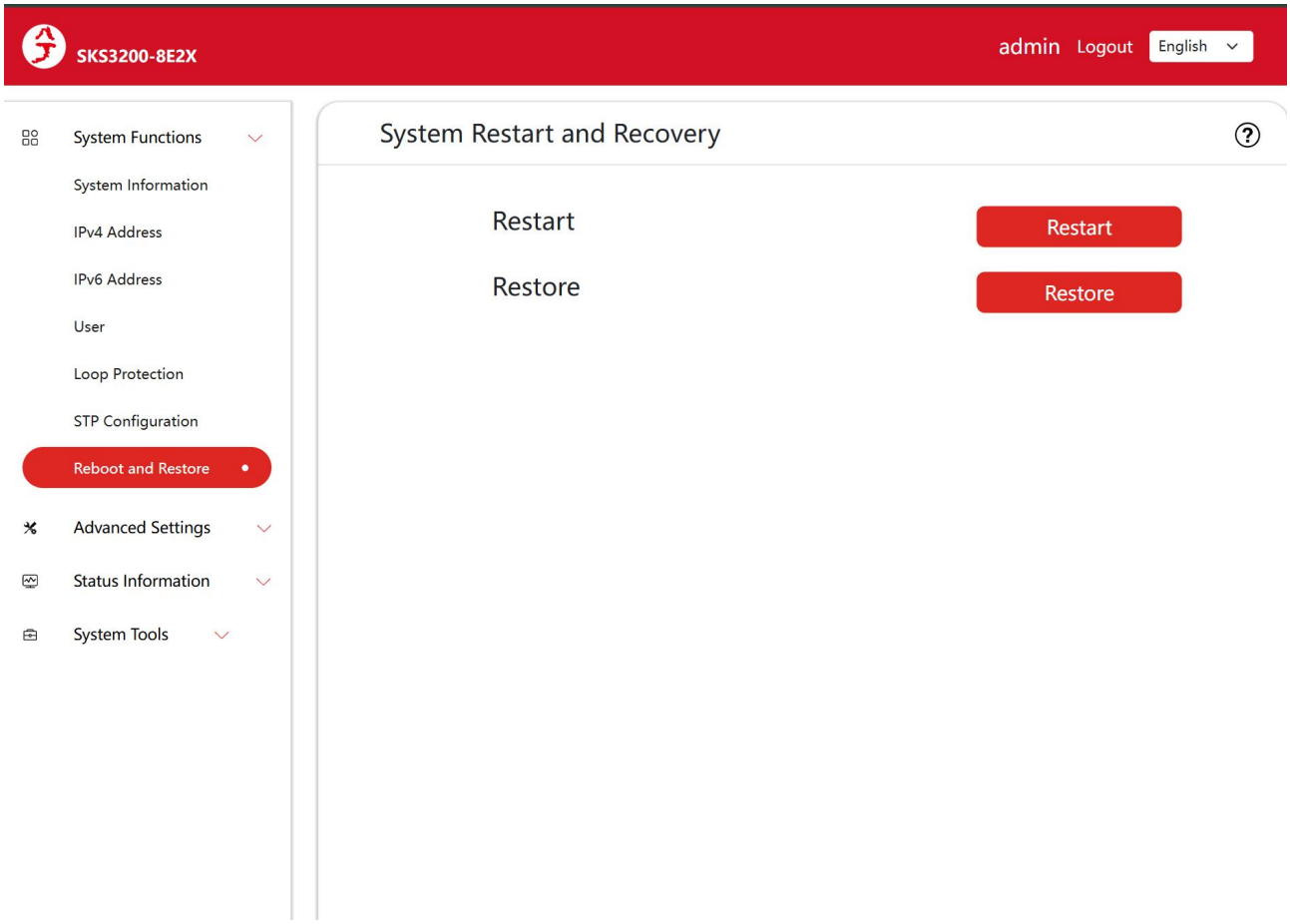

Figure 1-7. Restart and Restore

Use Restart to reboot the switch. Use Restore only when the current configuration is no longer required.

IMPORTANT: Restoring factory defaults removes the saved configuration and may interrupt network service. Back up the configuration before restoring the device.

2. Advanced Settings

2.1 Port Settings

Use the Port Settings page to configure port status, speed/duplex mode, and flow control.

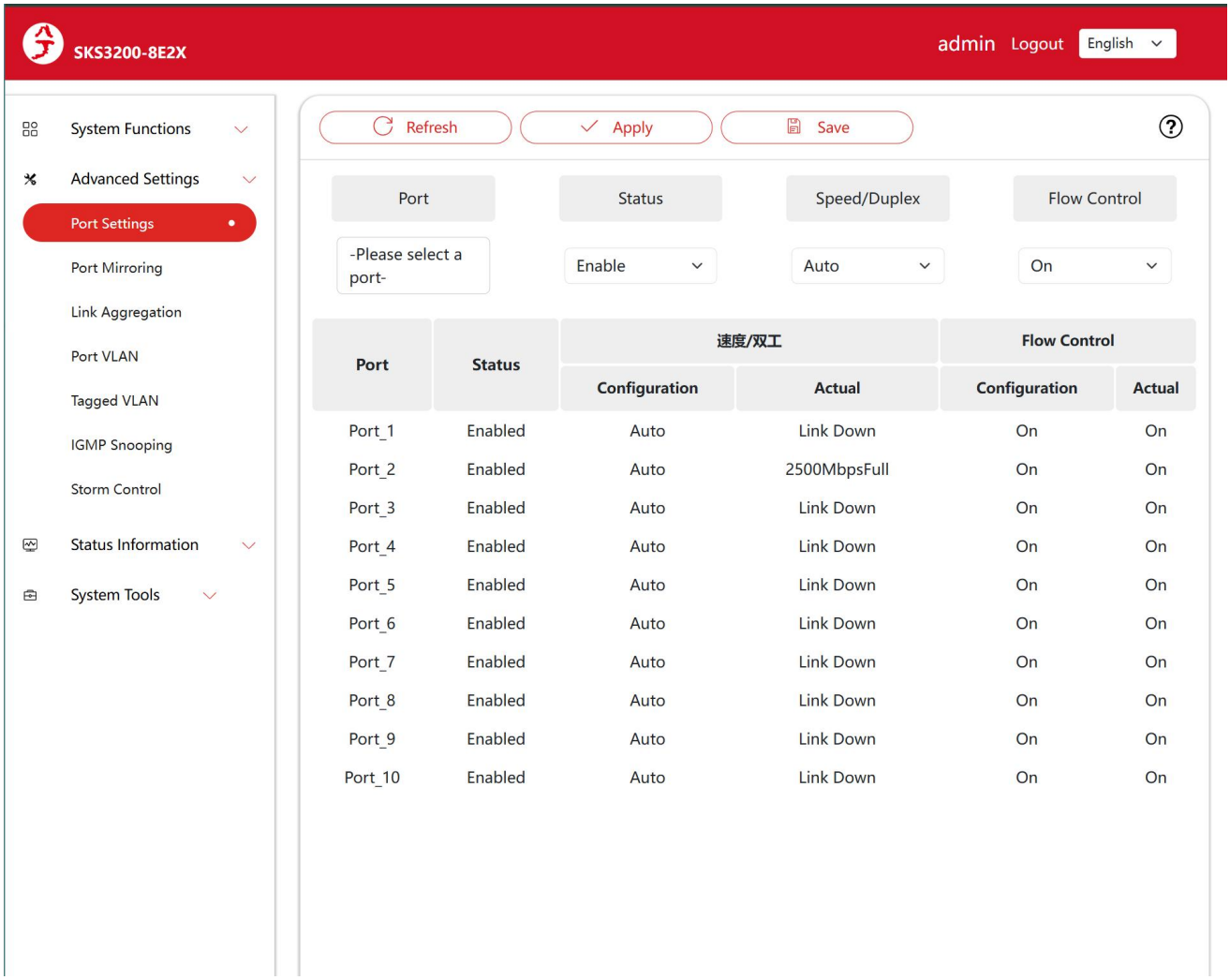

Figure 2-1. Port Settings

Select one or more ports, configure the operating state, speed/duplex mode, and flow control, then apply and save the configuration.

Item	Description
Port	Select the port to configure.
Status	Enabled: the port operates normally and forwards traffic. Disabled: the port is administratively shut down and does not forward traffic.
Speed/Duplex	Copper ports: 10 Mbps half duplex, 10 Mbps full duplex, 100 Mbps half duplex, 100 Mbps full duplex, 1000 Mbps full duplex, or 2500 Mbps full duplex. SFP/SFP+ ports: 1000 Mbps full duplex, 2500 Mbps full duplex, or 10 Gbps full duplex, subject to model and module support.
Flow Control	Enable or disable automatic traffic flow control.

2.2 Port Mirroring

Port mirroring copies packets from one or more source ports to a destination (monitor) port. A packet analyzer or monitoring appliance connected to the destination port can inspect traffic received or transmitted by the source ports for monitoring and troubleshooting. The switch supports one mirror group.

11. Select Advanced Settings > Port Mirroring.
12. Select the destination port and source port(s), then choose whether ingress traffic, egress traffic, or both directions are mirrored.

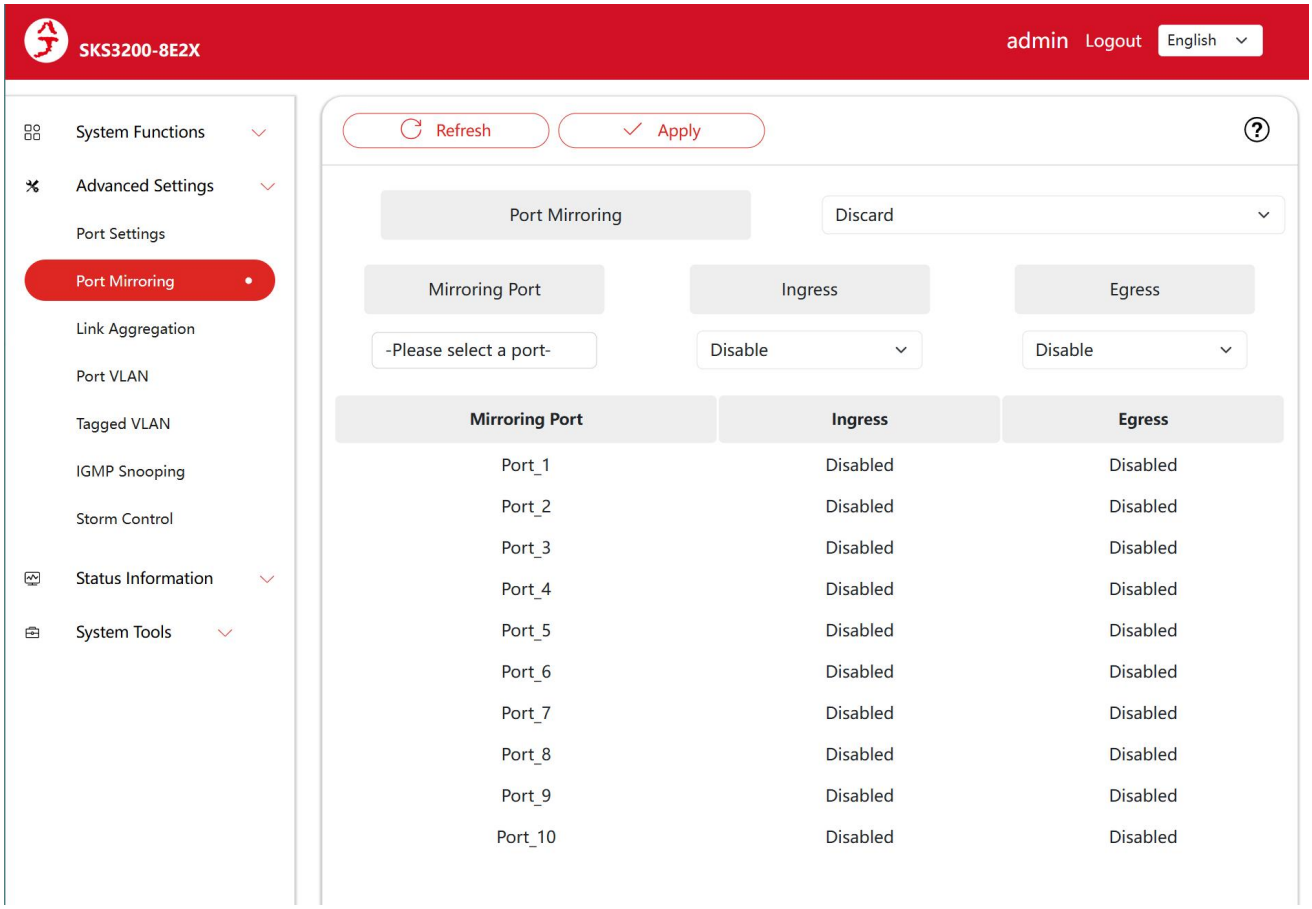

Figure 2-2. Port Mirroring

Choose the monitor port and the source ports. Enable ingress and/or egress mirroring for each source port, then apply and save the configuration.

Item	Description
Mirror Destination Port	Select the destination port connected to the monitoring device.
Mirrored Port	Select the source port whose traffic will be copied.
Ingress	Enable or disable mirroring of traffic received by the source port.
Egress	Enable or disable mirroring of traffic transmitted by the source port.

2.3 Link Aggregation

Link aggregation combines multiple physical Ethernet interfaces into one logical interface to increase bandwidth and improve link reliability. A Link Aggregation Group (LAG), also referred to as an Eth-Trunk, can distribute traffic across its member links and provide redundancy if a member link fails.

In the example below, three physical links between Switch A and Switch B form one Eth-Trunk. The logical link provides the combined bandwidth of the member links and maintains connectivity if an individual member link fails.

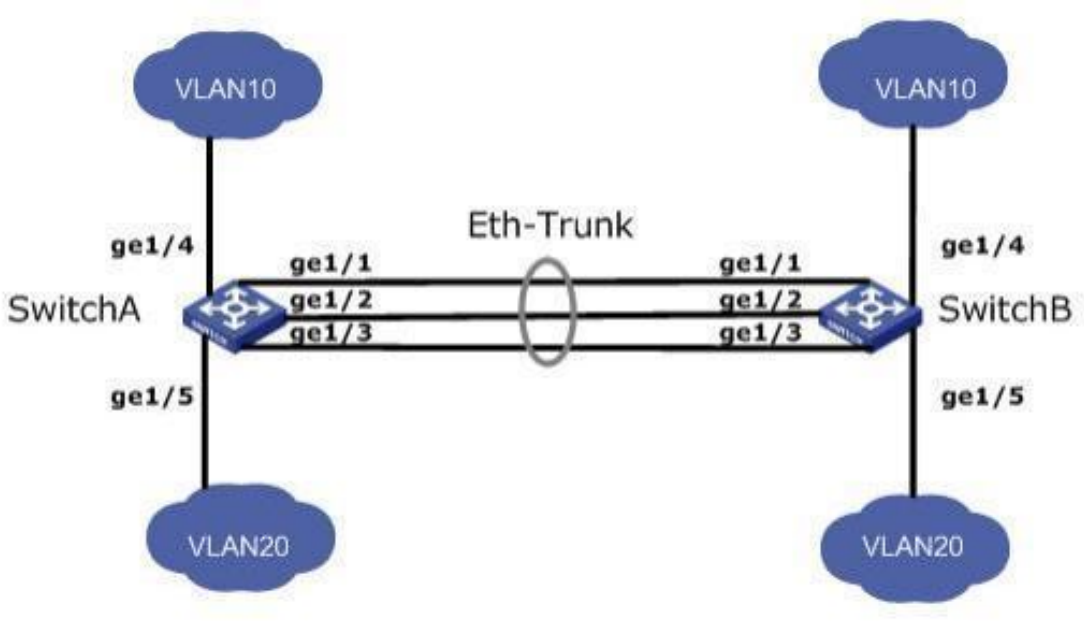

Figure 2-3. Link Aggregation Topology

Three physical links are bundled into one Eth-Trunk between two switches. Configure compatible aggregation settings at both ends of the link.

13. Select Advanced Settings > Link Aggregation.
14. Configure the aggregation mode, group, port priority, and LACP timeout where applicable.

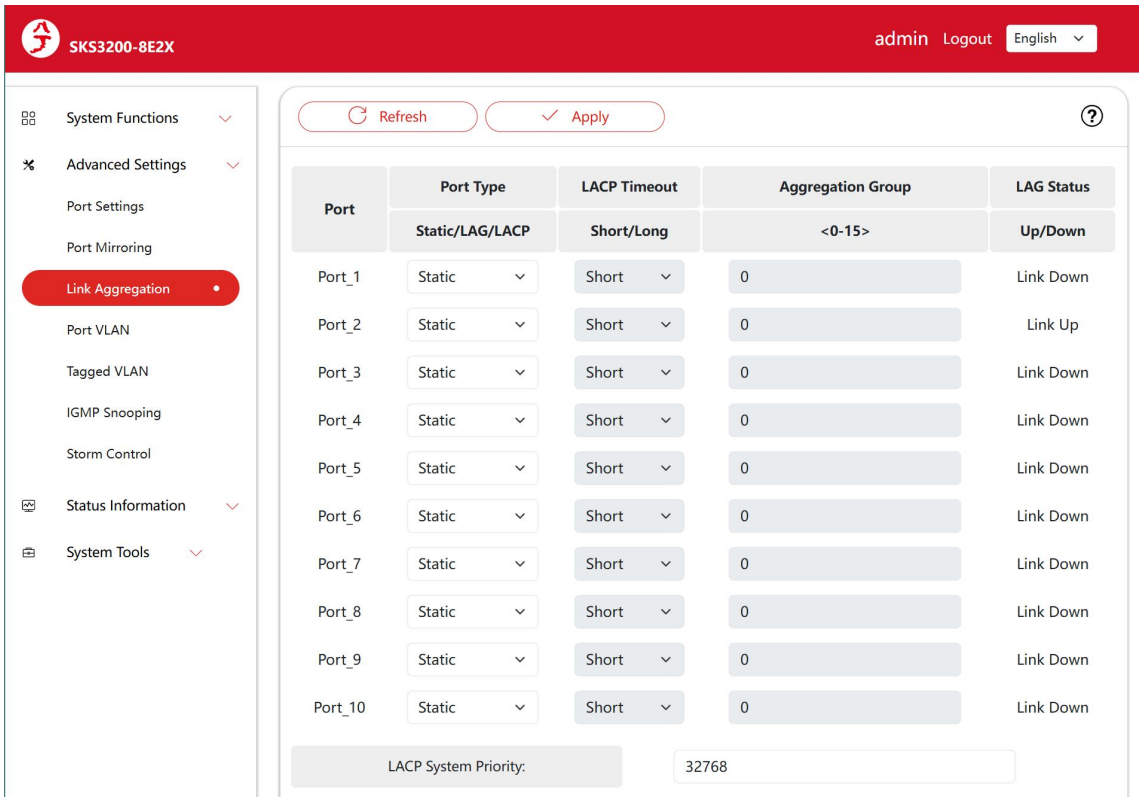

Figure 2-4. Link Aggregation Settings

Assign ports to a static LAG or an LACP group. All member ports should use compatible speed, duplex, and VLAN settings.

Item	Description
Port	Physical port number.
Port Type	Static: no aggregation by default. LAG: static link aggregation. LACP: dynamic aggregation using the Link Aggregation Control Protocol.
Priority	Port priority used by the aggregation protocol.
LACP Timeout	Long timeout: 90 seconds. Short timeout: 3 seconds.
Aggregation Group	Up to 16 groups are supported.
LAG Status	Displays the connection or aggregation status of the port.

2.4 Port-based VLAN

The switch supports multiple independent Layer 2 broadcast domains by assigning the same Port VLAN ID (PVID) to ports in the same group. Ports with the same PVID can communicate when the VLAN tagging rules also match; ports in different PVID groups are isolated unless traffic is routed or otherwise bridged by the network design.

15. Select Advanced Settings > Port VLAN.
16. Assign a PVID and accepted frame type to each port, then apply and save the configuration.

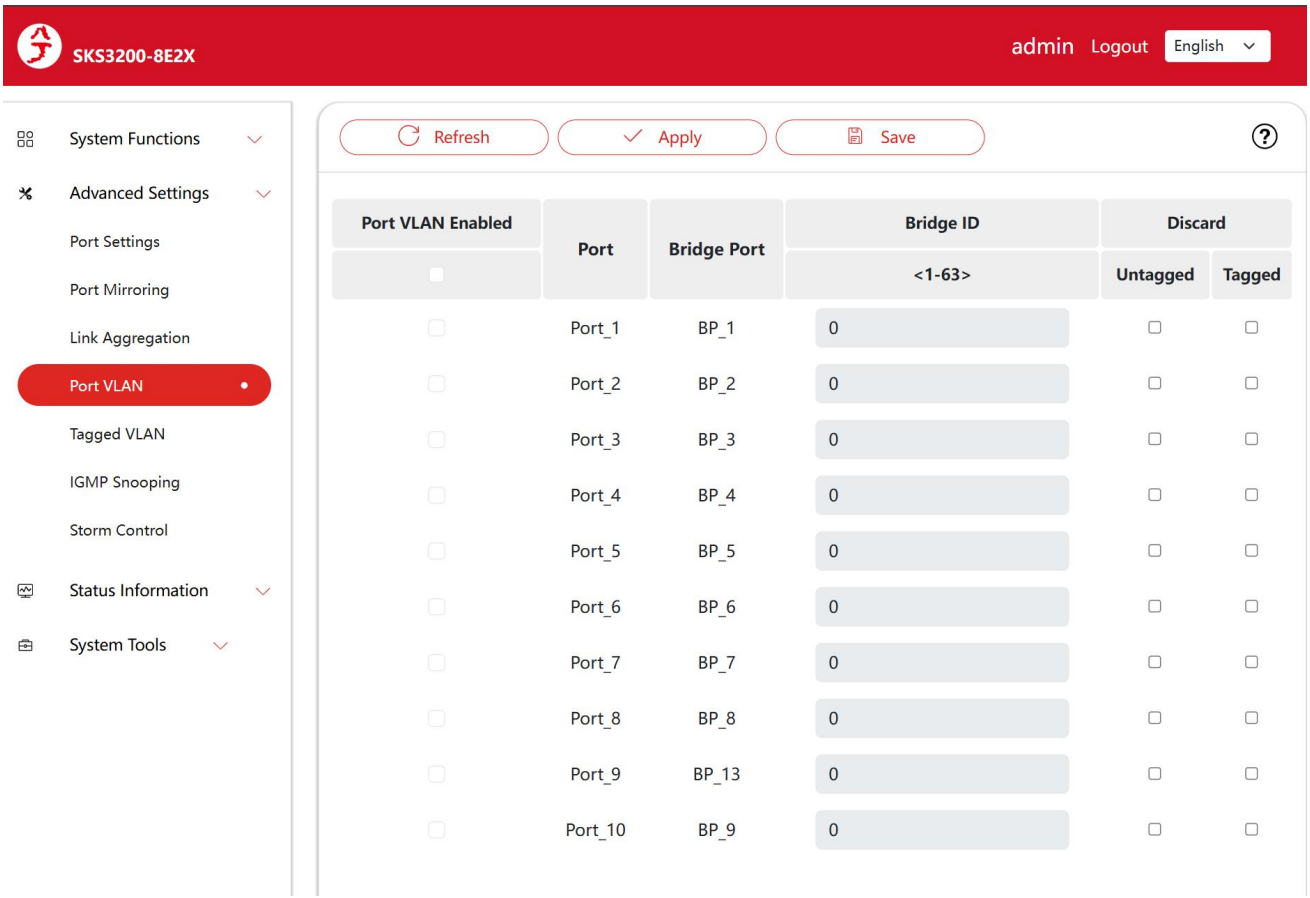

Figure 2-5. Port-based VLAN Settings

Assign PVID values and define which frame types each port accepts. Ports sharing a PVID are placed in the same port-based broadcast domain.

Item	Description
Port	Switch port that supports Port-based VLAN (PBV) configuration.
PVID	Port VLAN ID. Ports with the same PVID belong to the same broadcast domain.
Accepted Frame Type - All	Accept both tagged and untagged frames.
Accepted Frame Type - Tagged Only	Accept tagged frames only.
Accepted Frame Type - Untagged Only	Accept untagged frames only.
Refresh	Refresh the current page.
Apply	Apply the new settings.
Save	Save the current configuration.

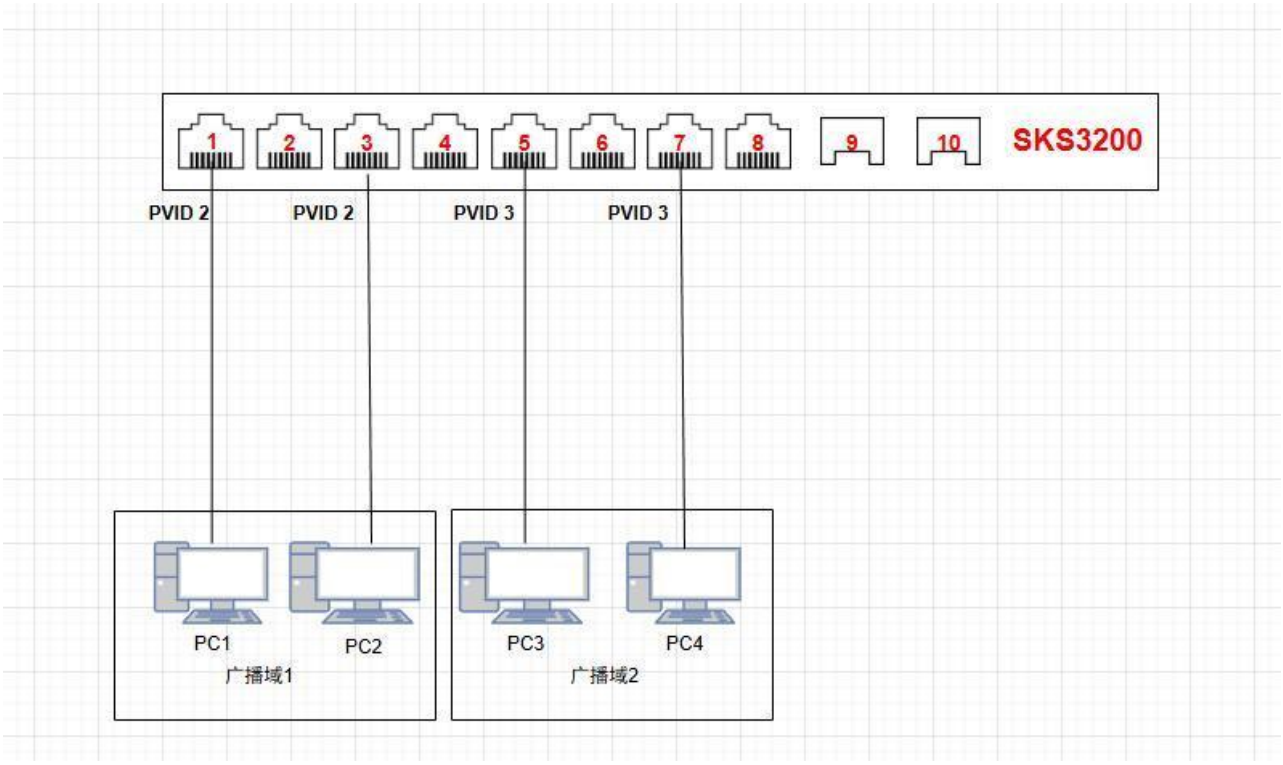

Figure 2-6. Port-based VLAN Configuration Result

This page shows the resulting PVID and accepted-frame configuration for the switch ports.

The following topology illustrates endpoint groups assigned to separate PVIDs. Communication requires both compatible PVID membership and compatible VLAN IDs carried by the endpoints or uplink.

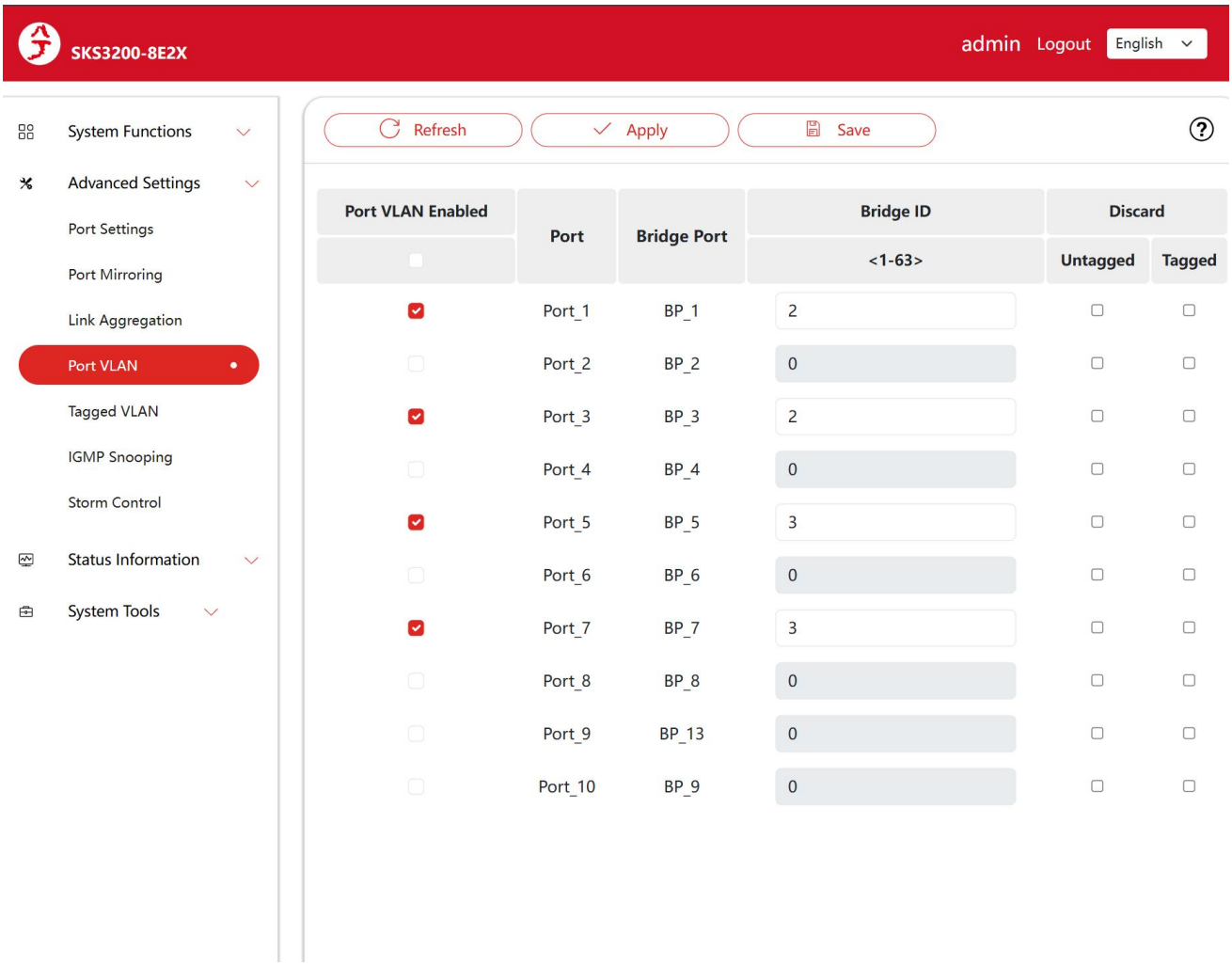

Figure 2-7. Port-based VLAN Topology

Example topology showing endpoints grouped by VLAN/PVID and an uplink used to carry the required traffic.

2.5 Tagged VLAN

The Tagged VLAN page lists the VLANs configured on the switch. A VLAN name is an administrative label and does not affect forwarding. Member Ports belong to the VLAN. Tagged Ports forward frames with the VLAN tag retained, similar to an IEEE 802.1Q trunk. Untagged Ports transmit frames after the VLAN tag is removed, similar to an access port. Ports assigned a PVID on the Port VLAN page normally appear as untagged members of the corresponding VLAN.

17. Select Advanced Settings > Tagged VLAN.
18. Add or modify the VLAN ID, VLAN name, member ports, tagged ports, and untagged ports, then apply and save the settings.

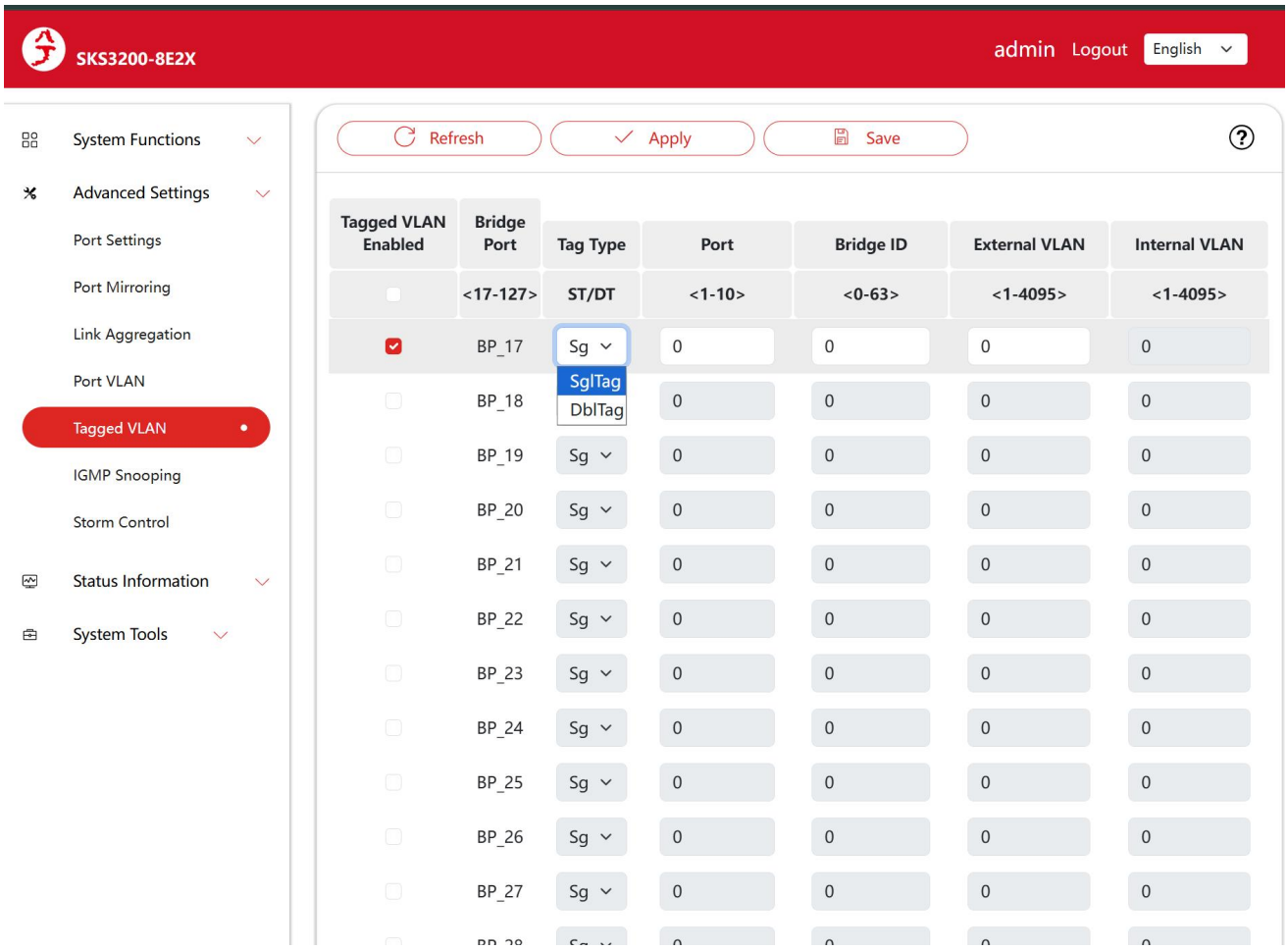

Figure 2-8. Tagged VLAN List

Review the configured VLAN IDs, names, membership, and tagging behavior. Use the available actions to modify or delete a VLAN.

Item	Description
VLAN ID	Numeric identifier of the VLAN.
VLAN Name	Optional administrative name or note for the VLAN.
Member Ports	Ports that belong to the VLAN.
Tagged Ports	Ports that forward frames with the current VLAN ID tag.
Untagged Ports	Ports that forward frames after the current VLAN tag is removed.
Operation	Modify or delete the selected VLAN.
Refresh	Refresh the current page.
Add	Create a VLAN and define its name, member ports, tagged ports, and untagged ports.
Apply	Apply the new settings.
Save	Save the current configuration.

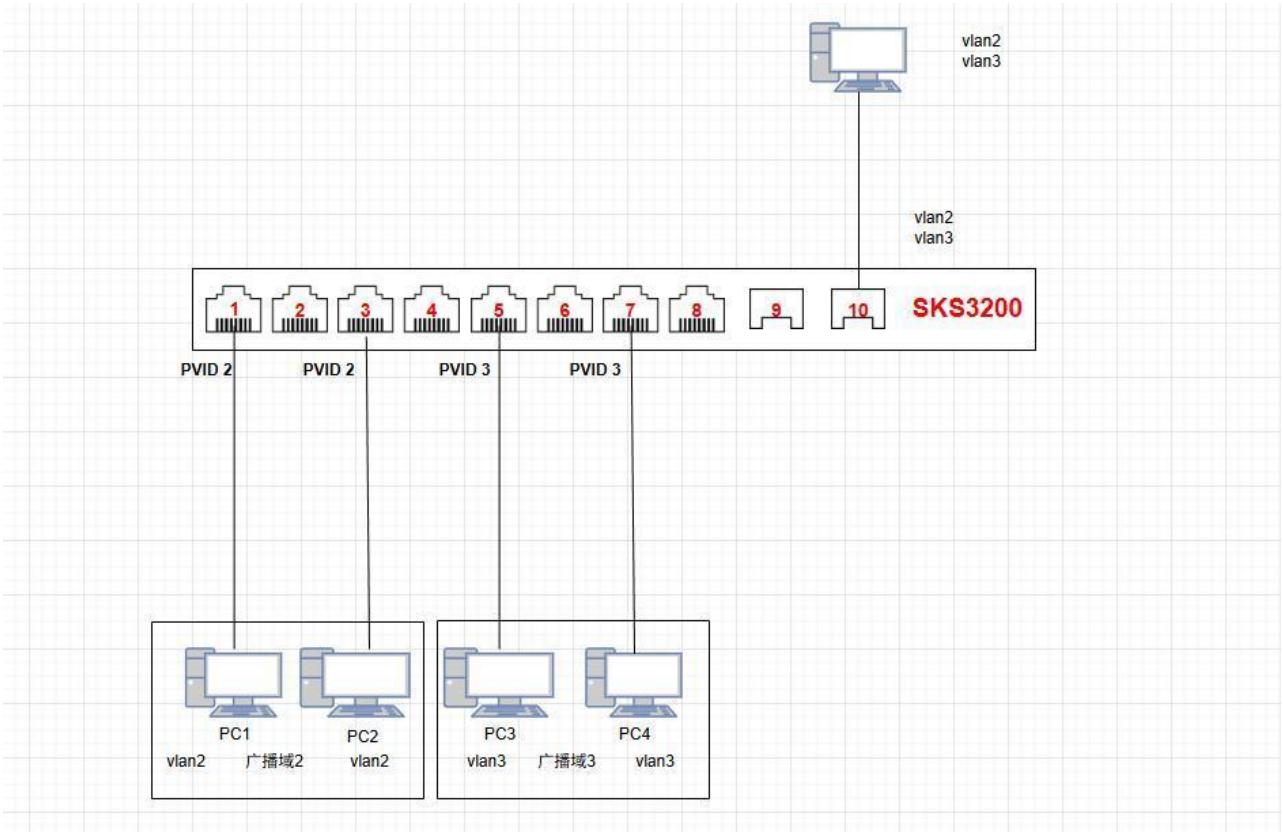

Figure 2-9. Tagged VLAN Topology

Example: ports 1, 3, and 10 carry VLAN 2; ports 5, 7, and 10 carry VLAN 3. Port 10 carries traffic for multiple VLANs and is configured as the tagged uplink.

2.6 IGMP Snooping

Internet Group Management Protocol (IGMP) snooping is a Layer 2 multicast control mechanism. The switch examines IGMP messages, builds mappings between ports and multicast MAC addresses, and forwards multicast data according to those mappings. Known multicast traffic is delivered only to interested receivers, while unknown multicast traffic may still be flooded within the VLAN.

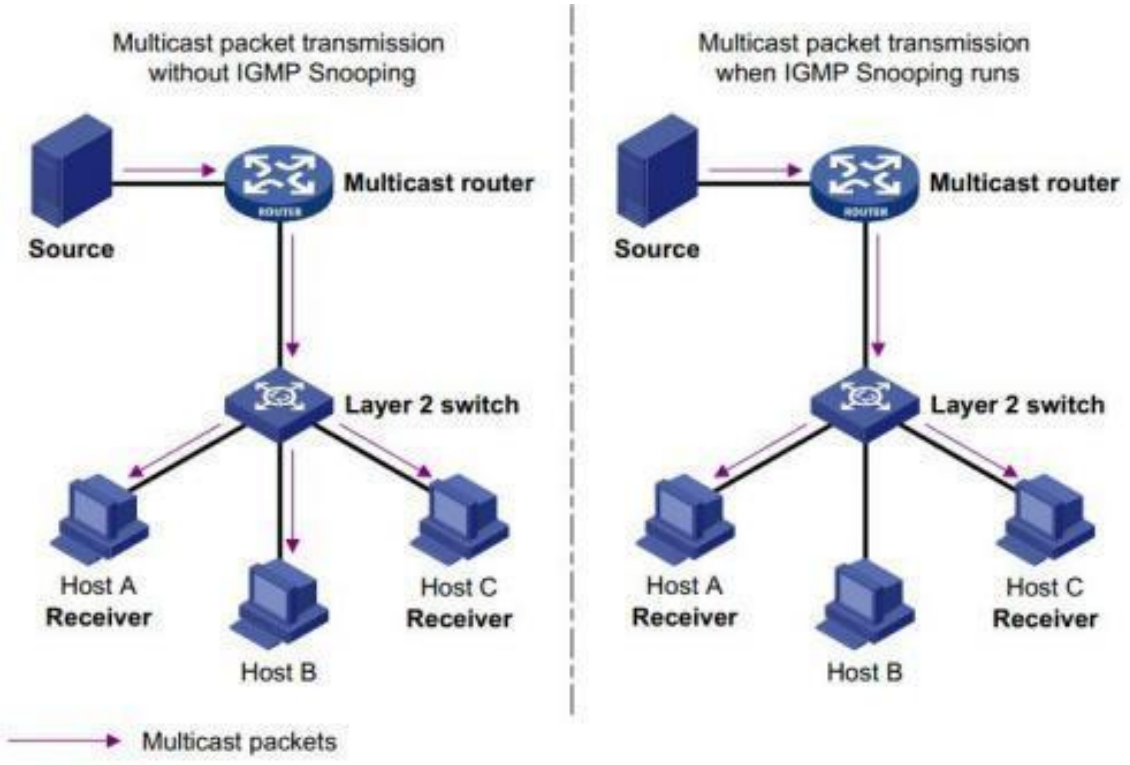

Figure 2-10. IGMP Snooping Forwarding Comparison

Without IGMP snooping, multicast traffic is flooded across the Layer 2 network. With IGMP snooping, known multicast traffic is forwarded only toward interested receivers.

19. Select Advanced Settings > IGMP Snooping.
20. Enable IGMP snooping before configuring the additional multicast options.

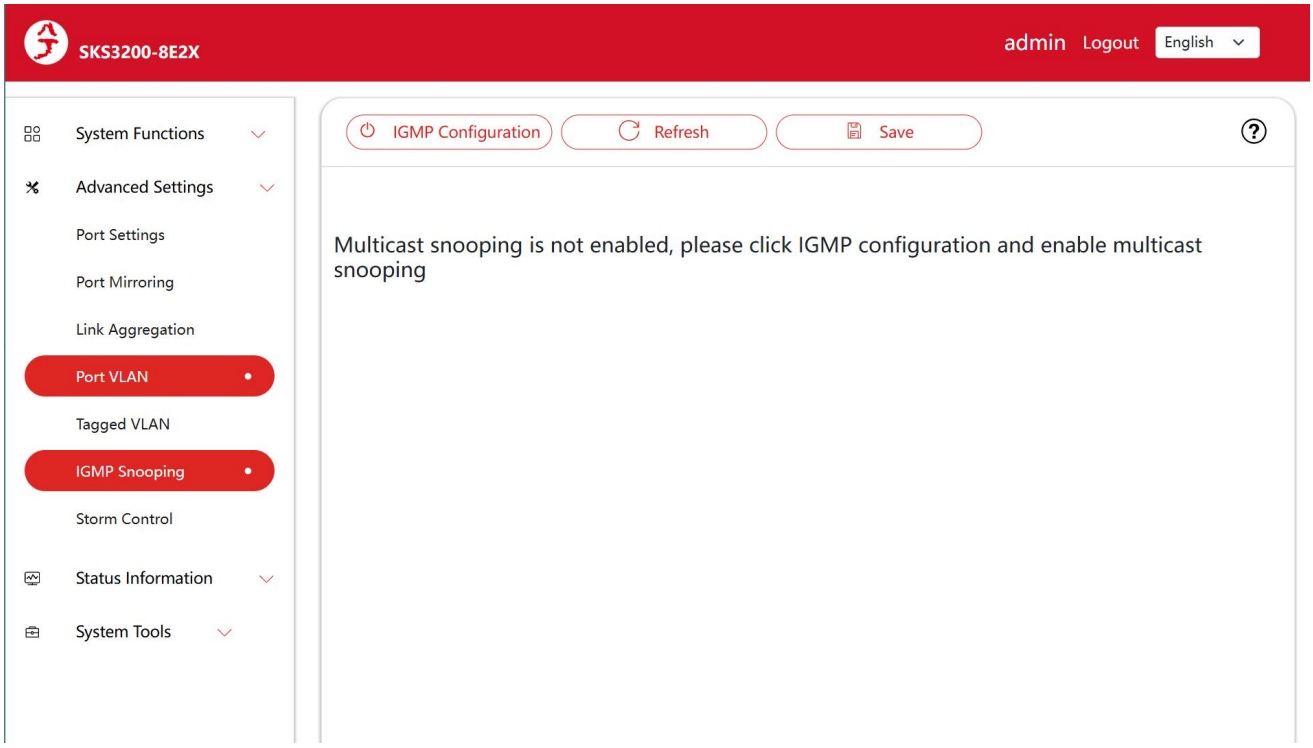

Figure 2-11. IGMP Snooping Status and Groups

View IGMP snooping status and the multicast group entries learned or configured by the switch.

Figure 2-12. IGMP Snooping Page

Open the IGMP configuration dialog and enable the required multicast features.

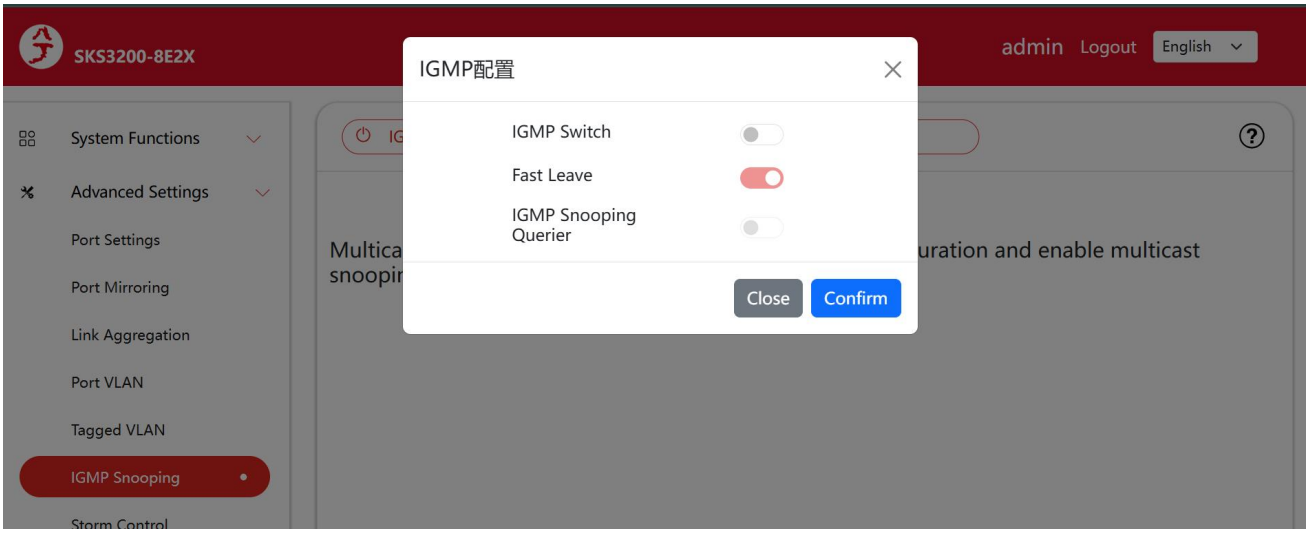

Figure 2-13. IGMP Configuration

Enable IGMP snooping, Fast Leave, or the join-message broadcast option as required by the multicast application.

Item	Description
IGMP Switch	Enable or disable IGMP snooping. Enabling the feature limits unnecessary multicast flooding and improves network efficiency.
Fast Leave	Enable or disable Fast Leave. When enabled, a port can be removed from a multicast group immediately after a leave event; use only where appropriate for the connected receiver topology.
Broadcast Join Message	Broadcast the message used to join a multicast group.

2.7 Storm Control

21. Select Advanced Settings > Storm Control.
22. Configure the traffic storm-control parameters for the required ports and traffic types, then apply and save the configuration.

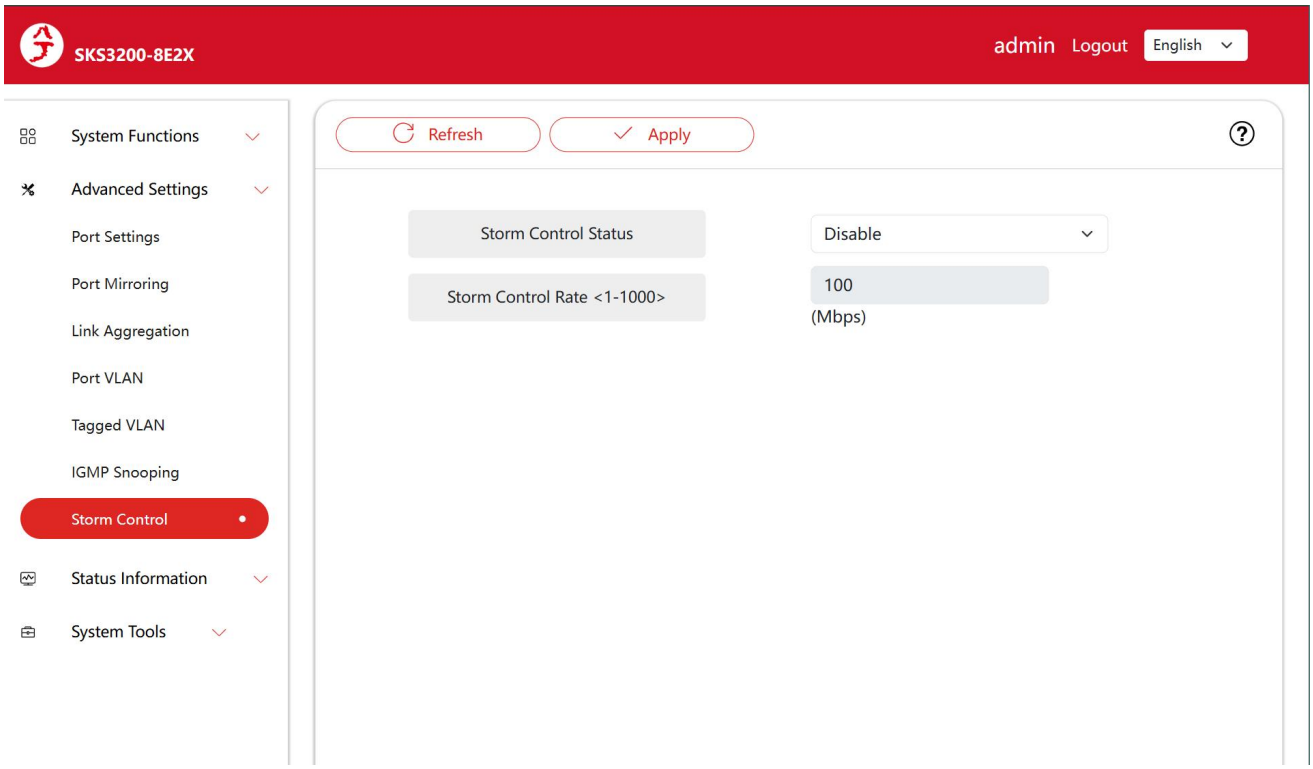

Figure 2-14. Storm Control

Use storm control to limit excessive broadcast, multicast, or unknown unicast traffic according to the options supported by the current firmware.

3. Status Information

3.1 Port Statistics

23. Select Status Information > Port Statistics.
24. Monitor port state and packet counters to troubleshoot connectivity and evaluate network performance.

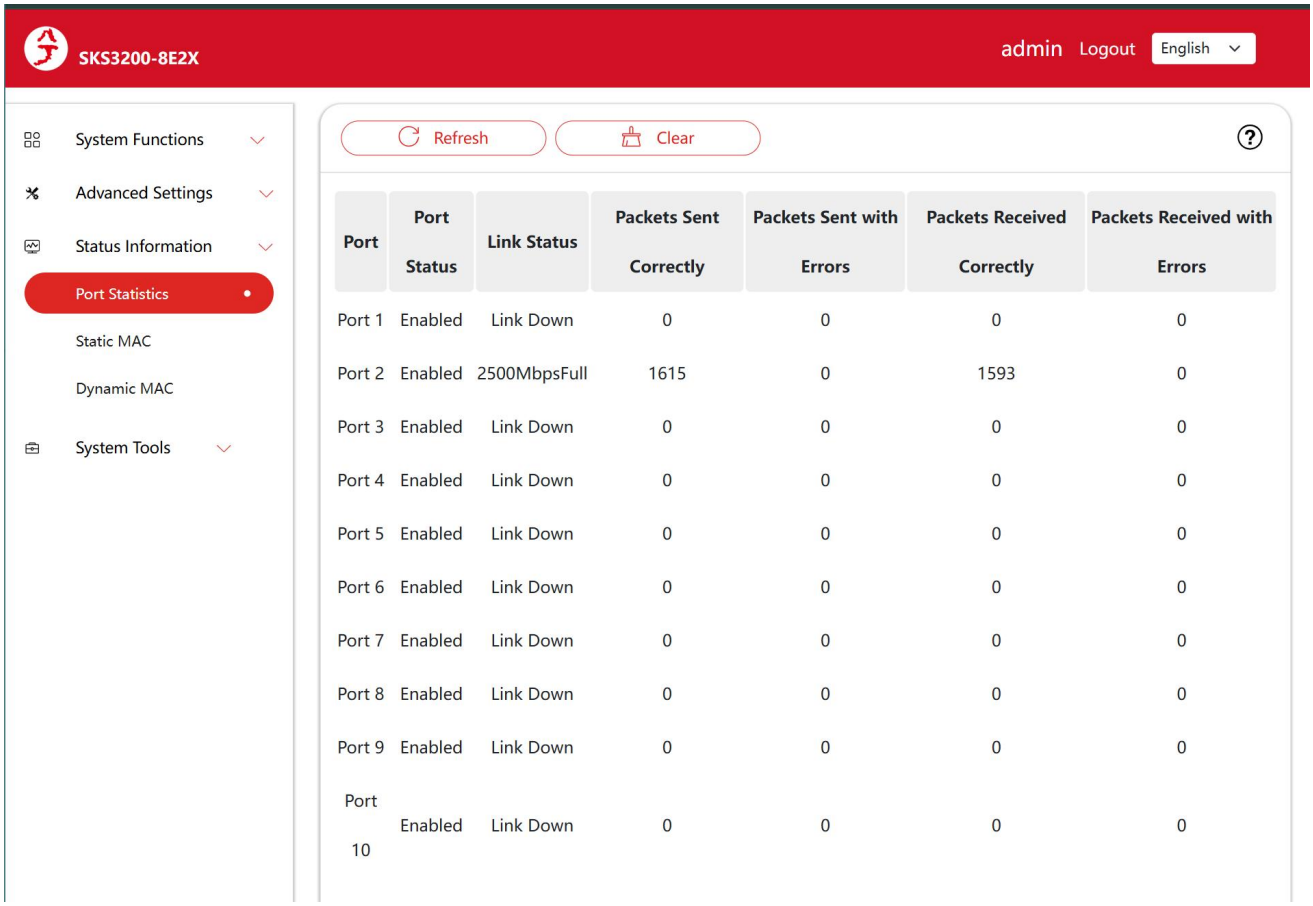

Figure 3-1. Port Statistics

Review link state, negotiated speed, and transmitted/received packet counters for each port. Refresh or clear the counters as required.

Item	Description
Administrative Status	Shows whether the port is enabled or disabled.
Port/Speed Status	Indicates the port link and negotiated speed status.
Link Status	Shows whether the link is connected and the negotiated link speed.
Tx Good Packets	Number of packets transmitted successfully.
Tx Error Packets	Number of packets transmitted with errors.
Rx Good Packets	Number of packets received successfully.
Rx Error Packets	Number of packets received with errors.
Refresh	Update the displayed port statistics.
Clear	Reset the displayed statistics to zero.
Save	Save the current configuration.

3.2 Static MAC

25. Select Status Information > Static MAC.

26. Add a static MAC address entry to the switch forwarding table and bind it to a specific port and VLAN where applicable.

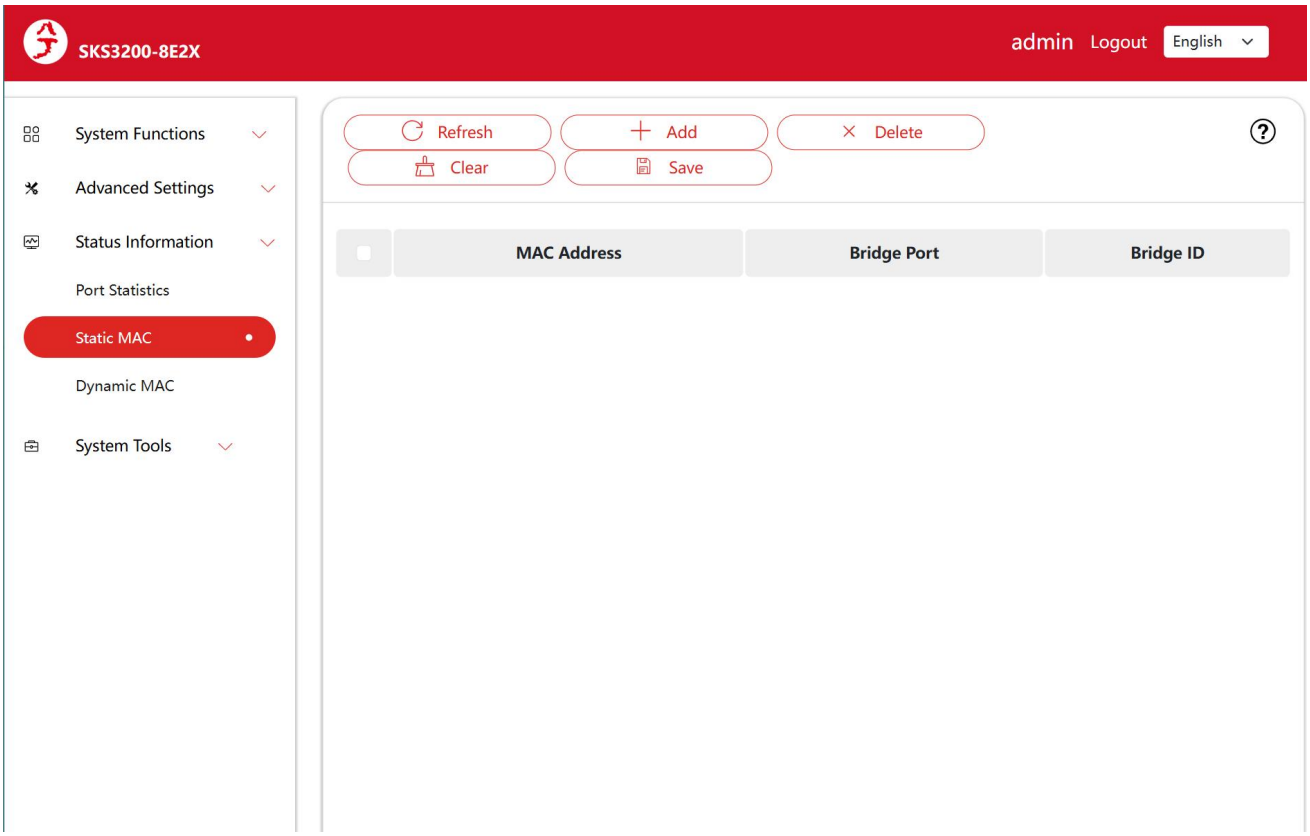

Figure 3-2. Static MAC Address Table

Add and manage static MAC address entries used for deterministic forwarding. Ensure the selected port and VLAN match the intended endpoint.

3.3 Dynamic MAC

27. Select Status Information > Dynamic MAC.
28. Display or search the MAC address entries currently learned by the switch.

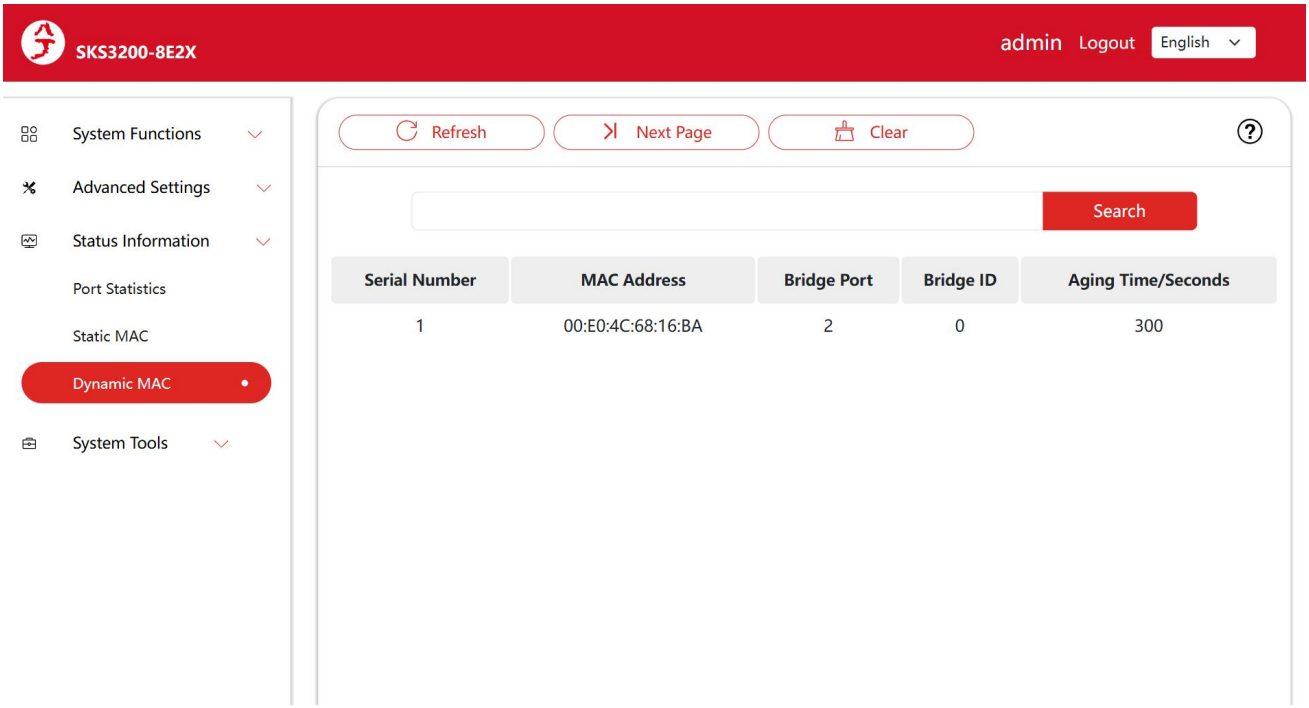

Figure 3-3. Dynamic MAC Address Table

Search and review learned MAC addresses, associated ports, VLAN IDs, and aging information.

Item	Description
Search	Search the MAC address table for a specific MAC address and VLAN ID.
Index	MAC address table entry index.
MAC Address	MAC address learned or recorded in the current table.
Port	Port associated with the MAC address.
VLAN ID	VLAN in which the MAC address was learned.
Aging Timer	Remaining lifetime of the learned MAC entry. The timer is refreshed by matching traffic; the default is 300 seconds.
Refresh	Refresh the entire MAC address table.
Clear	Clear the displayed dynamic MAC address entries.
Next Page	Display the next page of MAC address entries.
Save	Save the current configuration.

4. System Tools

4.1 Configuration Backup and Restore

29. Select System Tools > Configuration.
30. Download a backup of the current configuration or upload a previously saved configuration file.

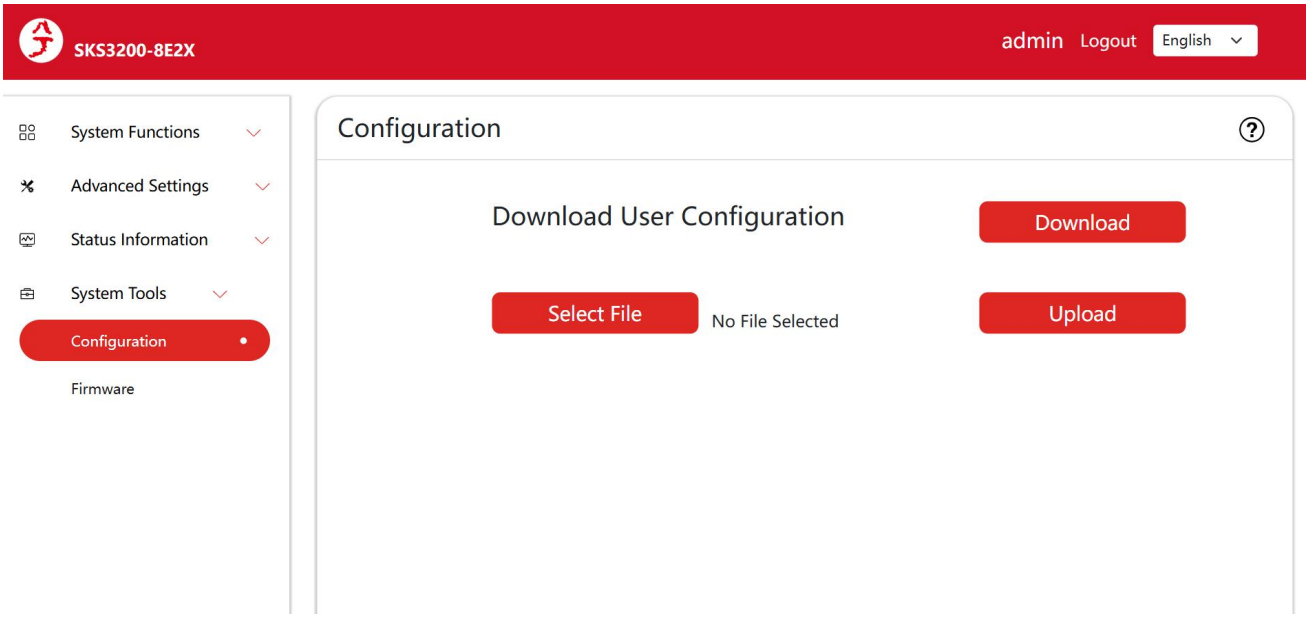

Figure 4-1. Configuration Backup and Restore

Download the active configuration for backup. Upload a compatible configuration file to restore previously saved settings.

Item	Description
Download Configuration	Download the current configuration settings.
Upload Configuration	Upload a configuration file to restore previously saved settings.

IMPORTANT: Keep configuration backups for each device and firmware branch. Upload only a configuration file compatible with the target model and firmware.

4.2 Firmware Upgrade

31. Select System Tools > Firmware.
32. Select the correct firmware file for the exact switch model and start the upgrade.

After the firmware has been programmed successfully, the switch restarts automatically. Back up the configuration before upgrading firmware.

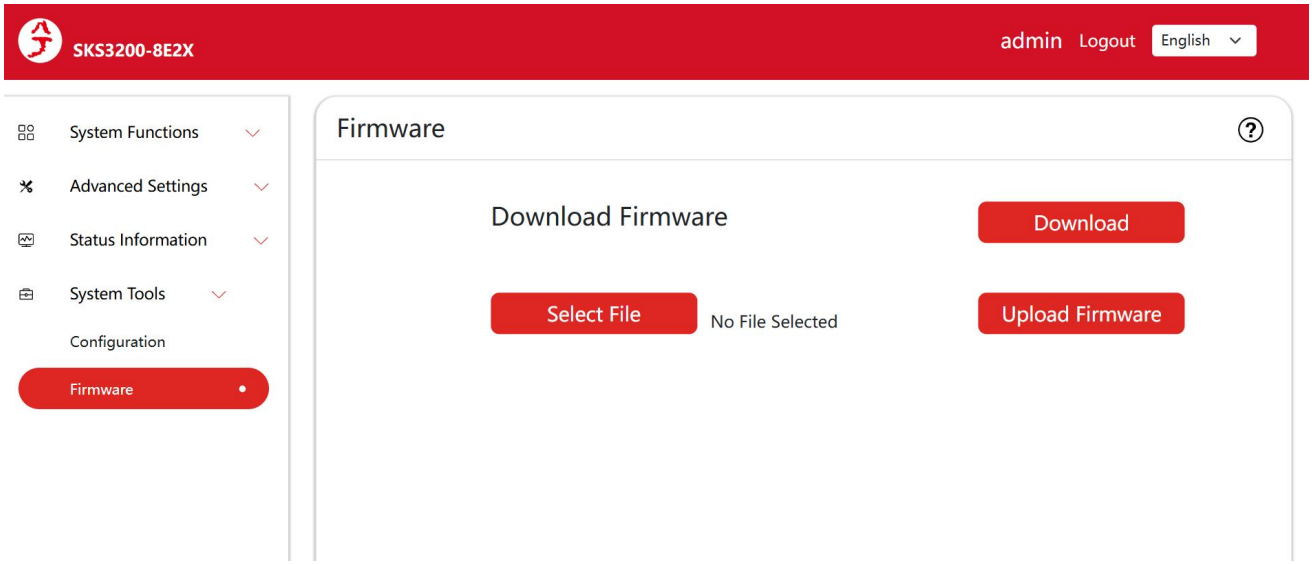

Figure 4-2. Firmware Upgrade

Upload the approved firmware package for the exact model. Allow the upgrade and automatic restart to finish before accessing the switch again.

IMPORTANT: Do not disconnect power, close the upgrade session, or interrupt network connectivity while firmware is being written. An interrupted upgrade can damage the device software.