Configuration Guide

For Packet Content ACL

T2600G Series Switch

1910012373 REV1.0.0

March 2018

CONTENTS

1 Overview 1

1.1 Packet Content ACL Introduction 1

1.2 Configuration Points of Packet Content ACL 1

2 Configuration Example 3

2.1 Network Requirements 3

2.2 Analyze Packet Structure 4

2.3 Formulate Configuration Scheme 5

2.4 Configure Packet Content ACL on the Switch 7

2.4.1 Using the GUI 7

2.4.2 Using the CLI 12

This guide applies to:

T2600G-52TS v3 or above, T2600G-28TS v3 or above, T2600G-28MPS v3 or above, T2600G-28SQ v1 or above.

1 Overview

On the latest T2600G series switches, we developed a new feature: Packet Content ACL. This configuration guide detailedly introduces how to configure Packet Content ACL.

1.1 Packet Content ACL Introduction

Comparing with the basic ACL, such as MAC ACL and IP ACL, Packet Content ACL provides more flexible and accurate rules to filter packets.

Packet Content ACL defines rules based on the offset position, string mask and user-defined string. That is, you can use offset position and string mask to specify specific segments of a received packet and compare these segments with your pre-defined strings, then the matched packets will follow the filtering operation: Permit or Deny.

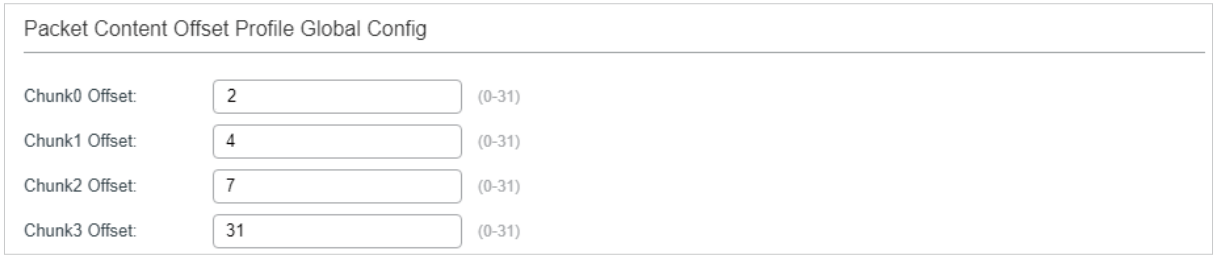
1.2 Configuration Points of Packet Content ACL

There are three necessary elements in Packet Content ACL: Chunk Offset, Chunk Value and Chunk Mask.

- **Chunk Offset**

Packet Content ACL can analyze up to four segments carried in the first 128 bytes of a received packet, and the length of each segment is 4 bytes. The Chunk Offset is used to specify the segments to be analyzed, as the following figure shows.

Figure 1-1 Chunk Offset

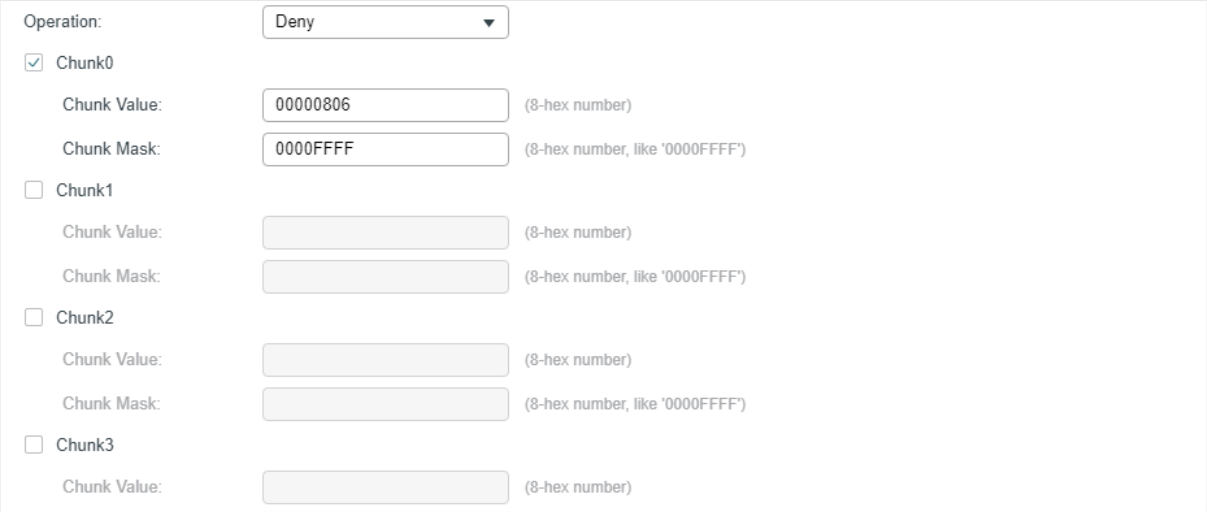


The valid values of Chunk Offset are from 0 to 31. Offset 31 specifies the 127th, 128th, 1st, 2nd bytes of the packet, offset 0 specifies the 3rd, 4th, 5th, 6th bytes of the packet, offset 1 specifies the 7th, 8th, 9th, 10th bytes of the packet, and so on, for the rest of the offset values.

- **Chunk Value and Chunk Mask**

As the above paragraph introduces, a Chunk Offset extracts a specific segment in a packet. Then, you need to configure a Chunk Mask to specify which fields of the extracted segment should be compared with the user-defined string, which is also called as Chunk Value.

Figure 1-2 Chunk Value and Chunk Mask



Taking the above rule as an example, Operation is **Deny**, Chunk0 Offset has been set to **2** in *Figure 1-2*, Chunk 0 is **enabled**, Chunk Value is **00000806**, and Chunk Mask is **0000FFFF**. The working mechanism of this rule is as follows:

1) The value of Chunk0 Offset **2** specifies the segment of a received packet: the 11th, 12th, 13th, 14th bytes. This 4-byte segment is extracted to be used for the following analysis.
2) The value of Chunk Mask **0000FFFF** indicates that the last 2 bytes (13th, 14th) of the extracted segment is to be compared with the Chunk Value **0806**.
3) If the 2-byte field in the packet is exactly 0806, the packet matches this rule. Then the filtering mode **Deny** is applied to this packet. If not, the switch uses the next rule to analyze this packet.

Note:

Both Chunk Mask and Chunk Value should be configured in Hexadecimal format.

Additionally, you can enable and configure the other three Chunks as well. Only a packet that matches all of the enabled Chunks in a rule is regarded to match this rule.

2 Configuration Example

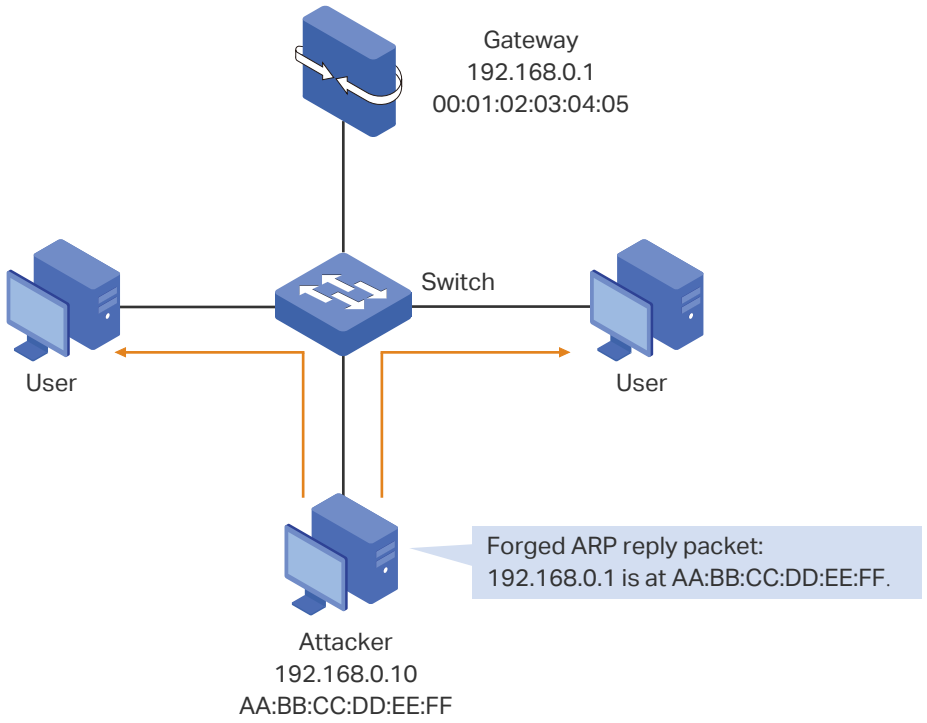
This chapter introduces how to configure Packet Content ACL through an example about ARP packet filtering. To complete the configuration, follow these steps:

1) Determine the network requirements.
2) Analyze the ARP packet structure.
3) Formulate the configuration scheme.
4) Configure Packet Content ACL on the switch.

2.1 Network Requirements

As the following figure shows, the IP address and MAC address of the legal Gateway are 192.168.0.1 and 00:01:02:03:04:05. An attacker in the LAN imitates the gateway to send forged ARP reply packets to users, so that these users record wrong ARP table and all packets to the internet are directed to the wrong node.

Figure 2-1 Network Topology



To protect the network from this kind of imitating gateway attacks, you can configure Packet Content ACL on the switch to filter forged ARP packets. The requirements are as follows:

When receives an ARP packet whose Sender IP Address is 192.168.0.1, the switch should check whether the Sender MAC Address is 00:01:02:03:04:05 or not. If yes, the packet is sent; if not, the packet is dropped.

2.2 Analyze Packet Structure

Before configuring Packet Content ACL, you first need to analyze the structure of the packets to be filtered, and then determine which segments should be extracted to be compared with the specific strings.

In this example, you need to analyze the ARP packet structure, as the following figure shows.

Figure 2-2 ARP Packet Structure

Destination Ethernet Address (first 2 bytes)	Destination Ethernet Address (next 2 bytes)	1st-4th bytes
Destination Ethernet Address (last 2 bytes)	Source Ethernet Address (first 2 bytes)	
Source Ethernet Address (next 2 bytes)	Offset 2 Source Ethernet Address (last 2 bytes)	9th-12th bytes
Offset 2 Frame Type	Hardware Type	
Protocol Type	Hardware Size / Protocol Size	
Operation	Offset 5 Sender MAC Address (first 2 bytes)	21st-24th bytes
Offset 5 Sender MAC Address (next 2 bytes)	Offset 6 Sender MAC Address (last 2 bytes)	25th-28th bytes
Offset 6 Sender IP Address (first 2 bytes)	Offset 7 Sender IP Address (last 2 bytes)	29th-32nd bytes
Offset 7 Target MAC Address (first 2 bytes)	Target MAC Address (next 2 bytes)	
Target MAC Address (last 2 bytes)	Target IP Address (first 2 bytes)	
Target IP Address (last 2 bytes)		

Consider the following three fields in the ARP packet: Frame Type, Sender MAC Address and Sender IP Address.

- **Frame Type**

Frame Type occupies the 13th, 14th bytes in the packet, so it can be specified by **Offset 2**, which indicates the 11th, 12th, 13th, 14th bytes.

The frame type of an ARP packet is 0806. Therefore, to identify ARP packets, the Chunk Mask and Chunk Value of Offset 2 should be set to **0000FFFF** and **00000806**.

- **Sender MAC Address and Sender IP Address**

Similarly, Sender MAC Address and Sender IP Address can be specified by **Offset 5, Offset 6** and **Offset 7**. In this example, the Sender MAC Address and Sender IP Address of the legal gateway are 00:01:02:03:04:05 and 192.168.0.1. To identify the ARP packets that are from the legal gateway, the Chunk Mask and Chunk Value should be set as follows:

Note:

Before calculating Chunk Mask and Chunk Value, transfer 192.168.0.1 from Decimal digit to Hexadecimal digit: C0A80001. For convenience, you can find a Hex converter on the internet.

Offset 5 specifies the first 4 bytes of Sender MAC Address. So the Chunk Mask and Chunk Value of Offset 5 should be set to **FFFFFFFF** and **00010203**.

Offset 6 specifies the last 2 bytes of Sender MAC Address and the first 2 bytes of Sender IP Address. So the Chunk Mask and Chunk Value of Offset 6 should be set to **FFFFFFFF** and **0405C0A8**.

Offset 7 specifies the last 2 bytes of Sender IP Address. So the Chunk Mask and Chunk Value of Offset 7 should be set to **FFFF0000** and **00010000**.

2.3 Formulate Configuration Scheme

Basing on the above analysis and network requirements, the configuration scheme for this example is as follows:

1) Configure Time Range.
2) Create a Packet Content ACL.
3) Configure the four Chunk Offset values as **2**, **5**, **6** and **7**.
4) Add a **Permit** rule for the Packet Content ACL.

   An ARP packet that contains the Sender IP Address 192.168.0.1 and Sender MAC Address 00:01:02:03:04:05 should be sent normally. The Chunk Offset configuration for this rule is shown in the following table.

   Table 2-1 Chunk Offset Configuration for the Permit Rule

Chunk Offset	Chunk Offset Value	Chunk Status	Chunk Mask	Chunk Value
Chunk0 Offset	2	Enable	0000FFFF	00000806
Chunk1 Offset	5	Enable	FFFFFFFF	00010203
Chunk2 Offset	6	Enable	FFFFFFFF	0405C0A8
Chunk3 Offset	7	Enable	FFFF0000	00010000

5) Add a **Deny** rule for the Packet Content ACL.

   An ARP packet that contains the Sender IP Address 192.168.0.1 and illegal Sender MAC Address, which is not 00:01:02:03:04:05, should be dropped. The Chunk Offset configuration for this rule is shown in the following table.

Table 2-2 Chunk Offset Configuration for the Deny Rule

Chunk Offset	Chunk Offset Value	Chunk Status	Chunk Mask	Chunk Value
Chunk0 Offset	2	Enable	0000FFFF	00000806
Chunk1 Offset	5	Disable	-	-
Chunk2 Offset	6	Enable	0000FFFF	0000C0A8
Chunk3 Offset	7	Enable	FFFF0000	00010000

6) Add a **Permit** rule for other packets. That is, if a packet that matches neither of the above rules, it should be sent normally.

Note:

The switch should first process the Permit rule to permit the packets from the legal gateway, and then the Deny rule to deny the packets from the attacker that claims to be the gateway. After that, the switch should permit other packets that match neither of the two rules.

Therefore, the Permit rule for ARP packets from the legal gateway should get the smallest rule ID, which means the highest priority. And so on, for the Deny rule and the other Permit rule.

7) Bind the Packet Content ACL to all ports of the switch.

2.4 Configure Packet Content ACL on the Switch

2.4.1 Using the GUI

Follow the steps below to configure Packet Content ACL:

1) Choose the menu **SYSTEM > Time Range > Time Range Config** and click Add to load the following page. Configure the time range name as Range1. Click Add in the **Period Time Config** section to add a period time and click **Create**.

Figure 2-3 Configuring Time Range

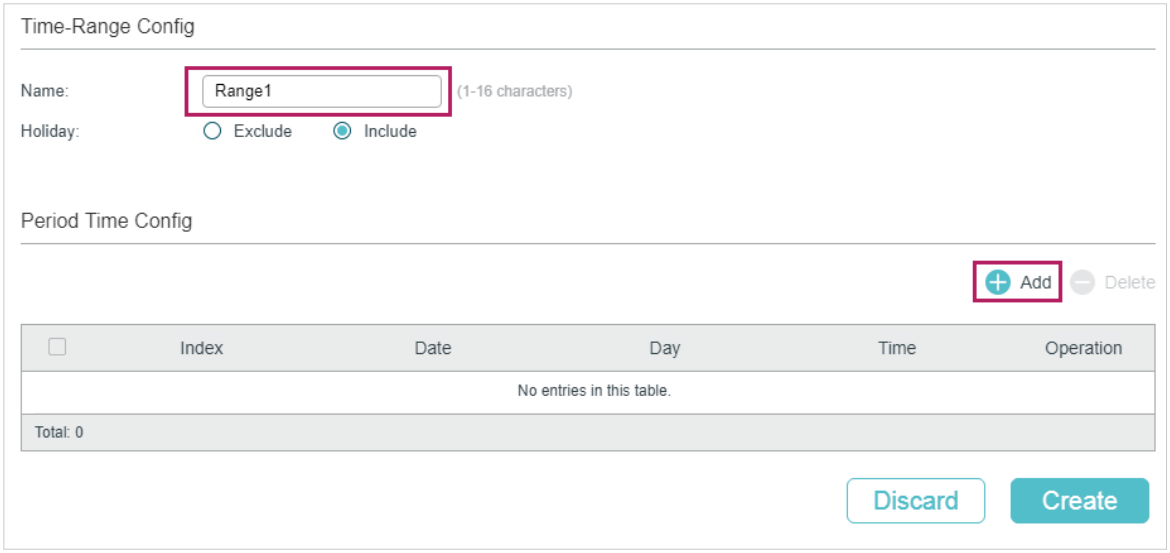
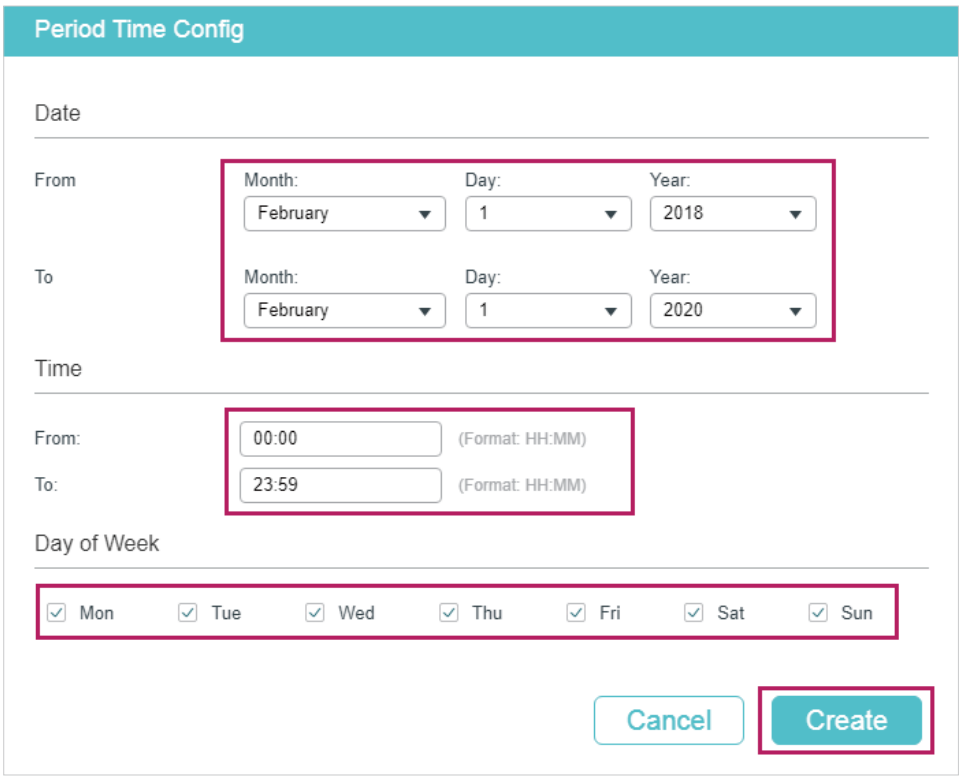
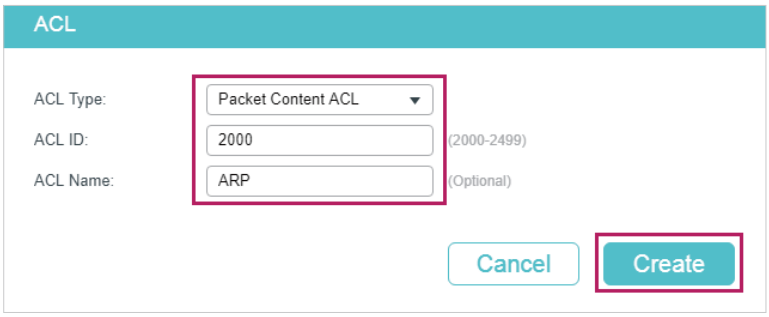


Figure 2-4 Adding Time Period Time



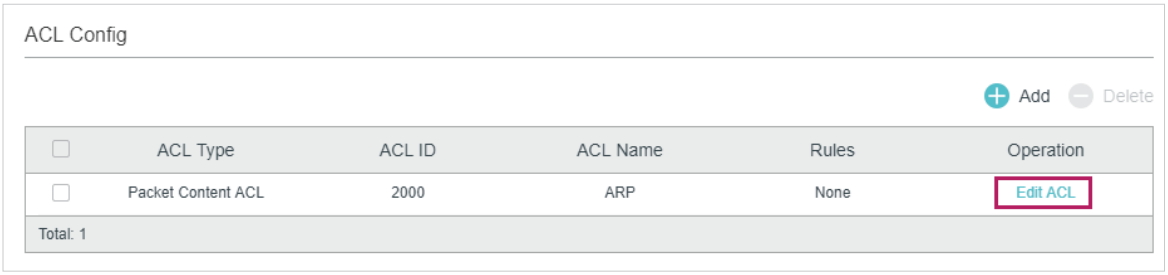
2) Choose the menu **SECURITY > ACL > ACL Config** and click Add to add a Packet Content ACL. Configure the ACL ID as 2000 and the ACL Name as ARP, and click **Create**.

Figure 2-5 Adding Packet Content ACL



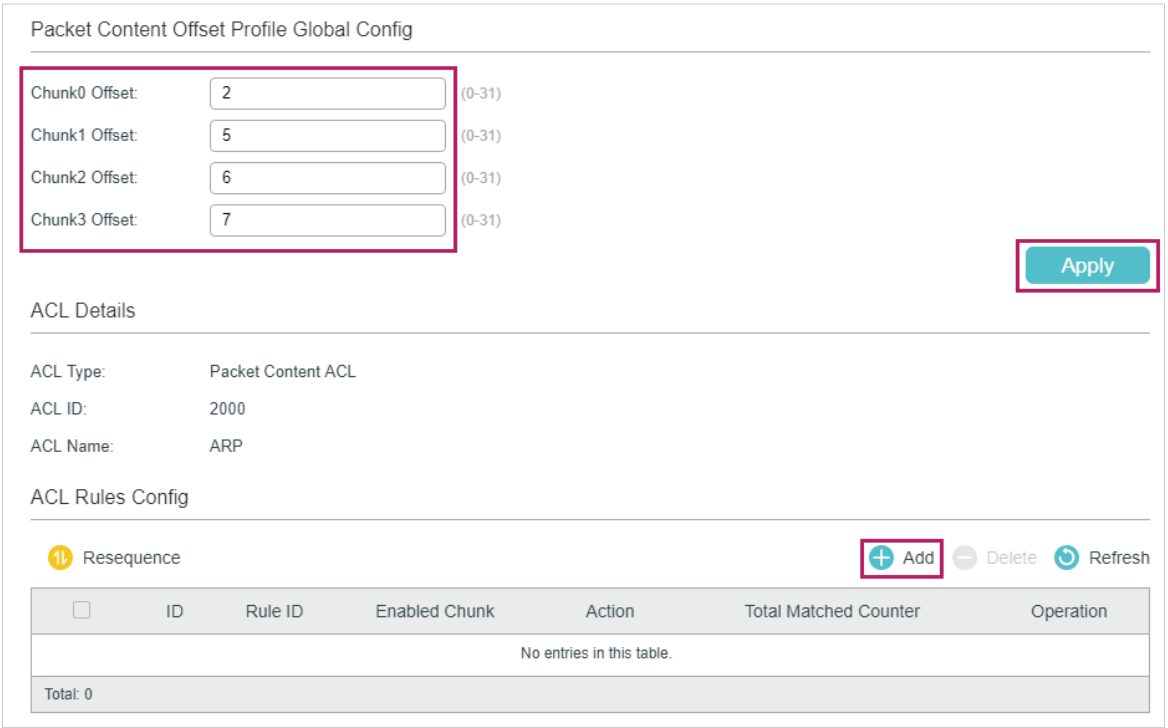
3) The added ACL is displayed in the table. Click **Edit ACL**.

Figure 2-6 Packet Content ACL Added



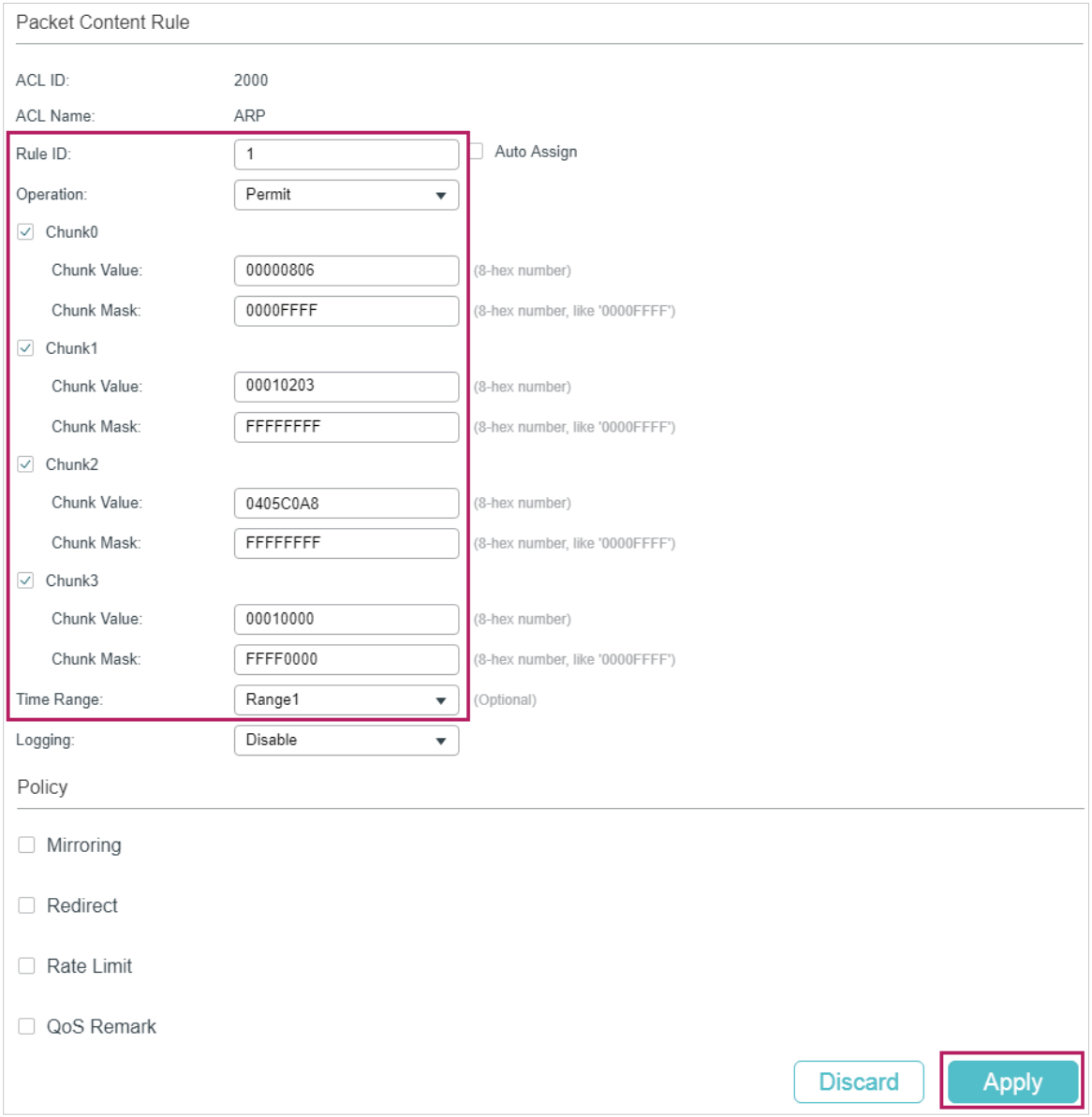
4) Set the four Chunk Offsets to 2, 5, 6 and 7, and click **Apply**. Then click Add in the **ACL Rules Config** section.

Figure 2-7 Editing Packet Content ACL



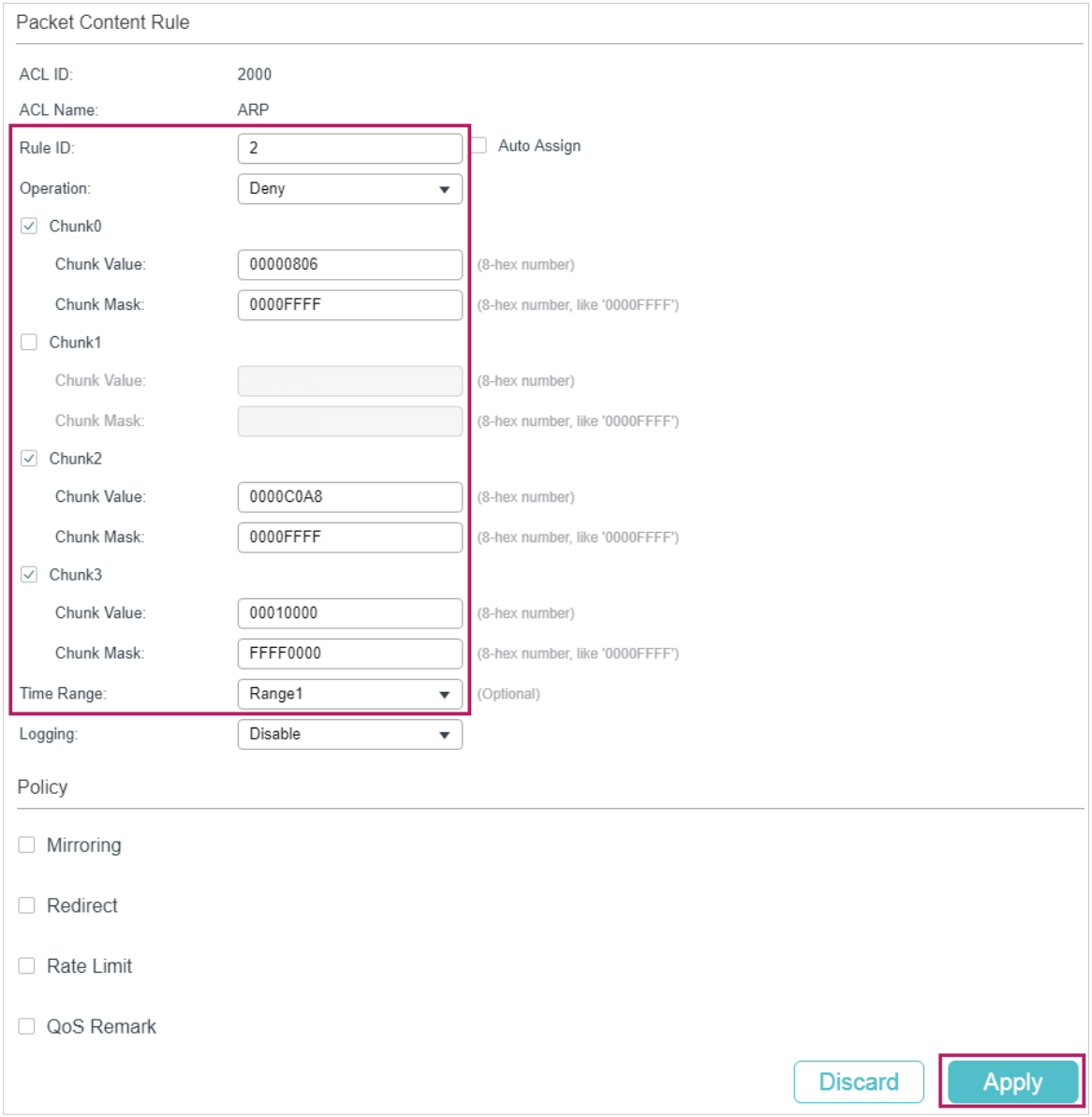
5) The following page will appear. Add the Permit rule for the packets that are from the legal gateway. Set Rule ID to 1, configure the four Chunk Offsets as *Table 2-1* lists, and select a Time Range. Click **Apply**.

Figure 2-8 Adding Permit Rule



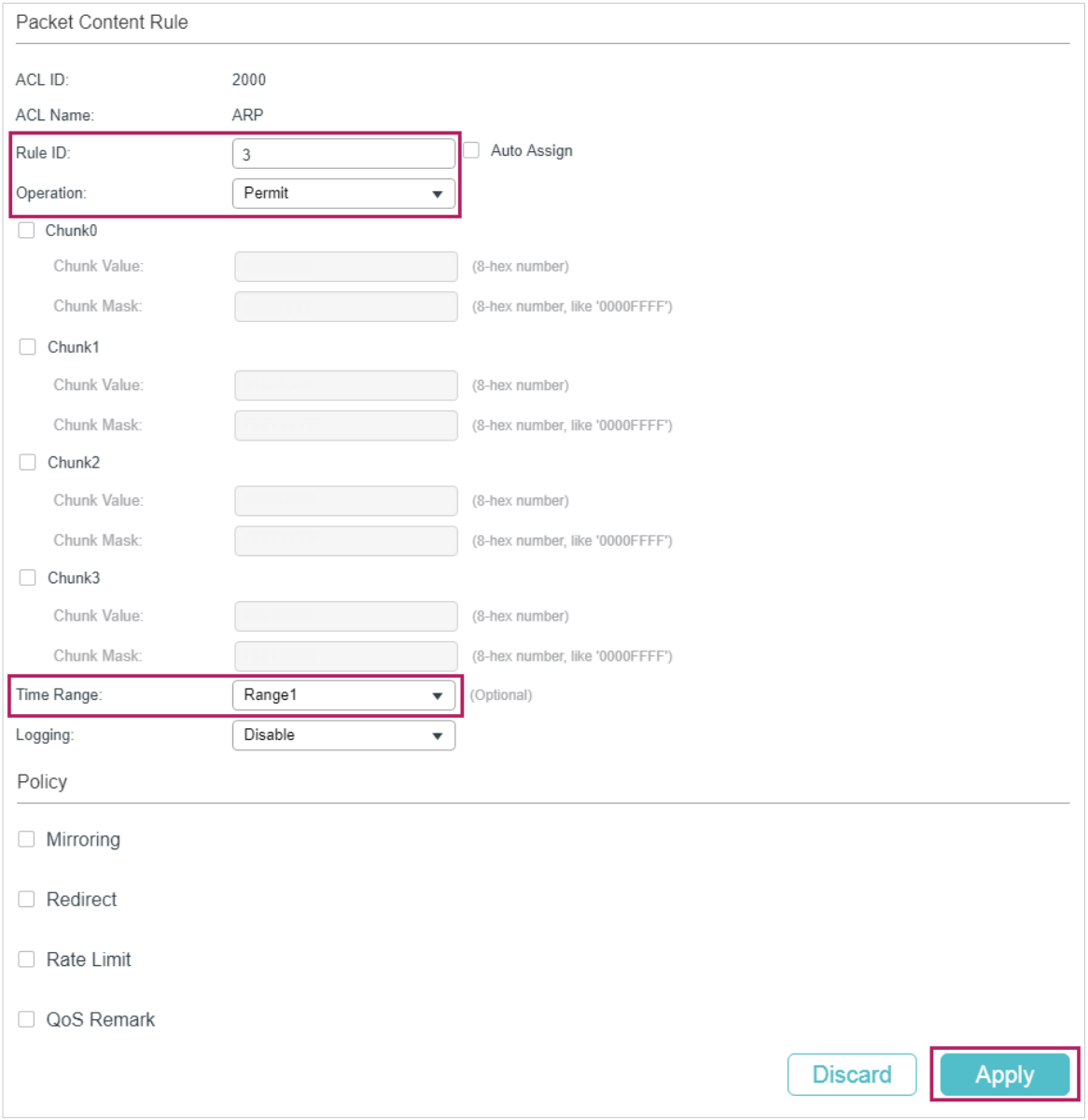
6) Similarly, add the Deny rule as *Table-2-2* lists. Set the Rule ID to 2 and select Time Range. Click **Apply**.

Figure 2-9 Adding Deny Rule



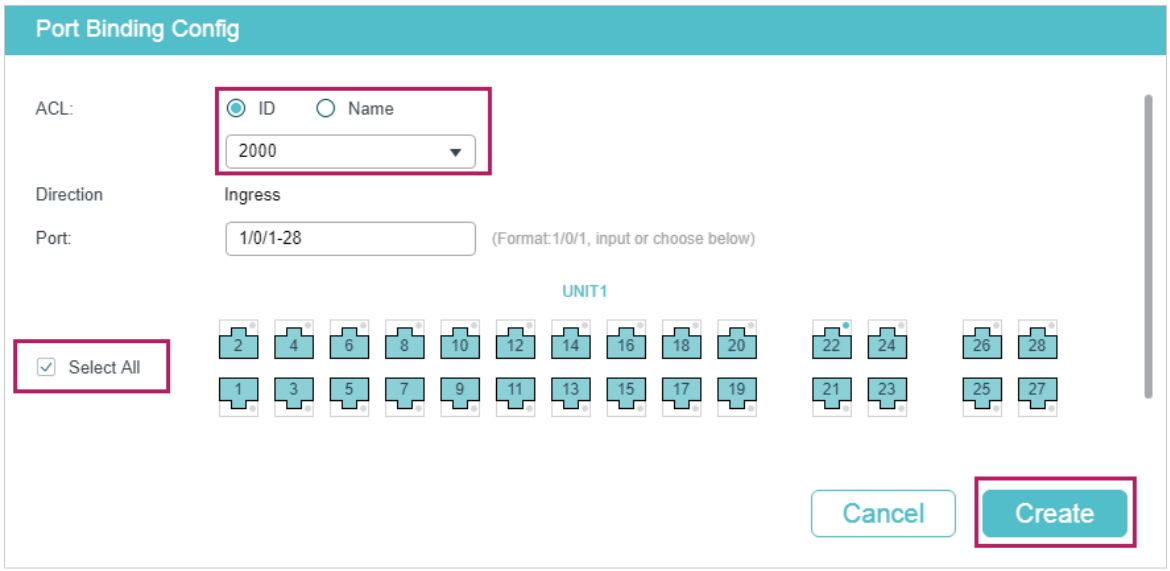
7) Similarly, add the Permit rule for the packets that match neither of the above two rules. Set the Rule ID to 3, remain the four Chunks as disabled and select Time Range. Click **Apply**.

Figure 2-10 Adding Deny Rule



8) Choose the menu **SECURITY > ACL > ACL Binding > Port Binding** and click Add to bind the Packet Content ACL to all ports of the switch. Select ACL 2000, check all ports, and click **Create**.

Figure 2-11 Binding ACL to Port



9) Click Save to save the configuration.

2.4.2 Using the CLI

Follow the steps below to configure Packet Content ACL:

1) Create a Time Range.

Switch#configure

Switch(config)#time-range Range1

Switch(config-time-range)#absolute from 02/01/2018 to 02/01/2020

Switch(config-time-range)#periodic start 00:00 end 23:59 day-of-the-week 1-7

Switch(config-time-range)#exit

2) Create a Packet Content ACL.

Switch(config)#access-list create 2000 name ARP

3) Set the four Chunk Offsets to 2, 5, 6 and 7.

Switch(config)#access-list packet-content profile chunk-offset0 2 chunk-offset1 5 chunk-offset2 6 chunk-offset3 7

4) Add the Permit rule for the packets that are from the legal gateway. Set the rule ID to 1, configure Chunk Offsets as *Table 2-1* lists, and bind Rang1 to this rule.

Switch(config)#access-list packet-content config 2000 rule 1 permit logging disable chunk0 00000806 mask0 0000ffff chunk1 00010203 mask1 ffffffff chunk2 0405c0a8 mask2 ffffffff chunk3 00010000 mask3 ffffffff tseg Range1

5) Add the Deny rule. Set the rule ID to 2, configure Chunk Offsets as *Table-2-2* lists, and bind Rang1 to this rule.

   Switch(config)#access-list packet-content config 2000 rule 2 deny logging disable chunk0 00000806 mask0 0000ffff chunk2 0000c0a8 mask2 ffffffff chunk3 00010000 mask3 ffff0000 tseg Range1

6) Add a Permit rule for the packets that matches neither of the above two rules. Set the rule ID to 3 and bind Rang1 to this rule.

   Switch(config)#access-list packet-content config 2000 rule 3 permit logging disable tseg Range1

7) View your settings.

   Switch(config)#show access-list 2000

   Packet content access list 2000 name: "ARP"

   rule 1 permit logging disable chunk0 00000806 mask0 0000FFFF chunk1 00010203 mask1 FFFFFFFF chunk2 0405C0A8 mask2 FFFFFFFF chunk3 00010000 mask3 FFFF0000 tseg "Range1"

   rule 2 deny logging disable chunk0 00000806 mask0 0000FFFF chunk2 0000C0A8 mask2 0000FFFF chunk3 00010000 mask3 FFFF0000 tseg "Range1"

   rule 3 permit logging disable tseg "Range1"

8) Save your settings.

   Switch(config)#end

   Switch#copy running-config startup-config

COPYRIGHT & TRADEMARKS