ACL Principles and Configuration



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



Contents

[1 ACL Principles and Configuration 1](#_Toc60149216)

[1.1 Foreword 1](#_Toc60149217)

[1.2 Objectives 1](#_Toc60149218)

[1.3 ACL Overview 2](#_Toc60149219)

[1.3.1 Background: A Tool Is Required to Filter Traffic 2](#_Toc60149220)

[1.3.2 ACL Overview 2](#_Toc60149221)

[1.4 Basic Concepts and Working Mechanism of ACLs 4](#_Toc60149222)

[1.4.1 ACL Composition 4](#_Toc60149223)

[1.4.2 Rule ID 5](#_Toc60149224)

[1.4.3 Wildcard (1) 6](#_Toc60149225)

[1.4.4 Wildcard (2) 7](#_Toc60149226)

[1.4.5 ACL Classification and Identification 8](#_Toc60149227)

[1.4.6 Basic and Advanced ACLs 9](#_Toc60149228)

[1.4.7 ACL Matching Mechanism 10](#_Toc60149229)

[1.4.8 ACL Matching Order and Result 11](#_Toc60149230)

[1.4.9 ACL Matching Position 12](#_Toc60149231)

[1.5 Basic Configurations and Applications of ACLs 14](#_Toc60149232)

[1.5.1 Basic Configuration Commands of Basic ACLs 14](#_Toc60149233)

[1.5.2 Case: Use a Basic ACL to Filter Data Traffic 15](#_Toc60149234)

[1.5.3 Basic Configuration Commands of Advanced ACLs 16](#_Toc60149235)

[1.5.4 Case: Use Advanced ACLs to Prevent User Hosts on Different Network Segments from Communicating 18](#_Toc60149236)

[1.6 Summary 20](#_Toc60149237)

[1.7 Quiz 21](#_Toc60149238)

# ACL Principles and Configuration

## Foreword

Rapid network development brings challenges to network security and quality of service (QoS). Access control lists (ACLs) are closely related to network security and QoS.

By accurately identifying packet flows on a network and working with other technologies, ACLs can control network access behaviors, prevent network attacks, and improve network bandwidth utilization, thereby ensuring network environment security and QoS reliability.

This course describes the basic principles and functions of ACLs, types and characteristics of ACLs, basic composition of ACLs, ACL rule ID matching order, usage of wildcards, and ACL configurations.

## Objectives

On completion of this course, you will be able to:

Describe the basic principles and functions of ACLs.

Understand the types and characteristics of ACLs.

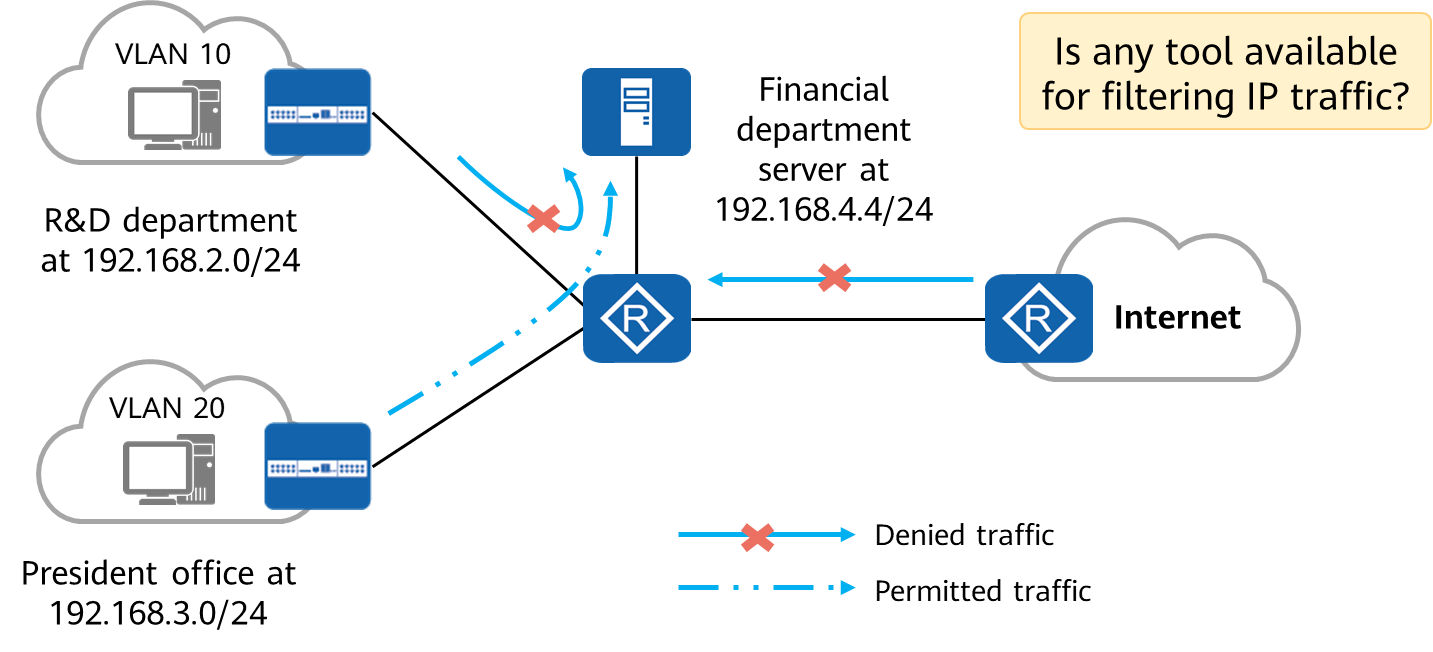
Describe the basic composition of ACLs and ACL rule ID matching order.

Understand how to use wildcards in ACLs.

Complete the basic configurations of ACLs.

## ACL Overview

### Background: A Tool Is Required to Filter Traffic



Background: A Tool Is Required to Filter Traffic

To ensure financial data security, an enterprise prohibits the R&D department's access to the financial department server but allows the president office's access to the financial department server.

Rapid network development brings the following issues to network security and QoS:

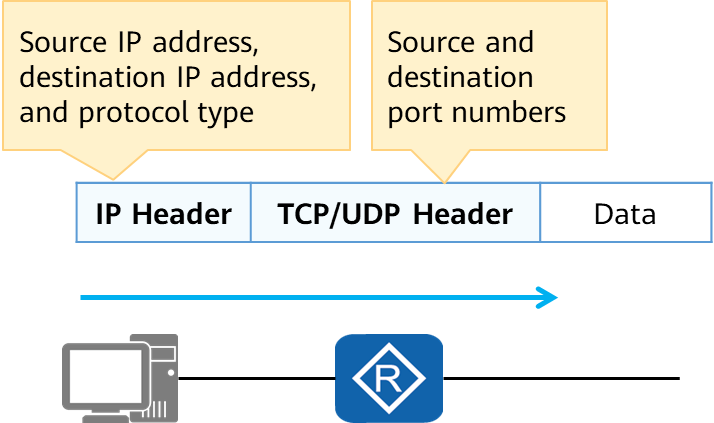
* Resources on the key servers of an enterprise are obtained without permission, and confidential information of the enterprise leaks, causing a potential security risk to the enterprise.
* The virus on the Internet spreads to the enterprise intranet, threatening intranet security.
* Network bandwidth is occupied by services randomly, and bandwidth for delay-sensitive services such as voice and video cannot be guaranteed, lowering user experience.

These issues seriously affect network communication, so network security and QoS need to be improved urgently. For example, a tool is required to filter traffic.

### ACL Overview

An ACL is a set of sequential rules composed of permit or deny statements.

An ACL matches and distinguishes packets.



ACL Overview

ACL application：

* Matching IP traffic
* Invoked in a traffic filter
* Invoked in network address translation (NAT)
* Invoked in a routing policy
* Invoked in a firewall policy
* Invoked in QoS
* Others

ACLs accurately identify and control packets on a network to manage network access behaviors, prevent network attacks, and improve bandwidth utilization. In this way, ACLs ensure security and QoS.

An ACL is a set of sequential rules composed of permit or deny statements. It classifies packets by matching fields in packets.

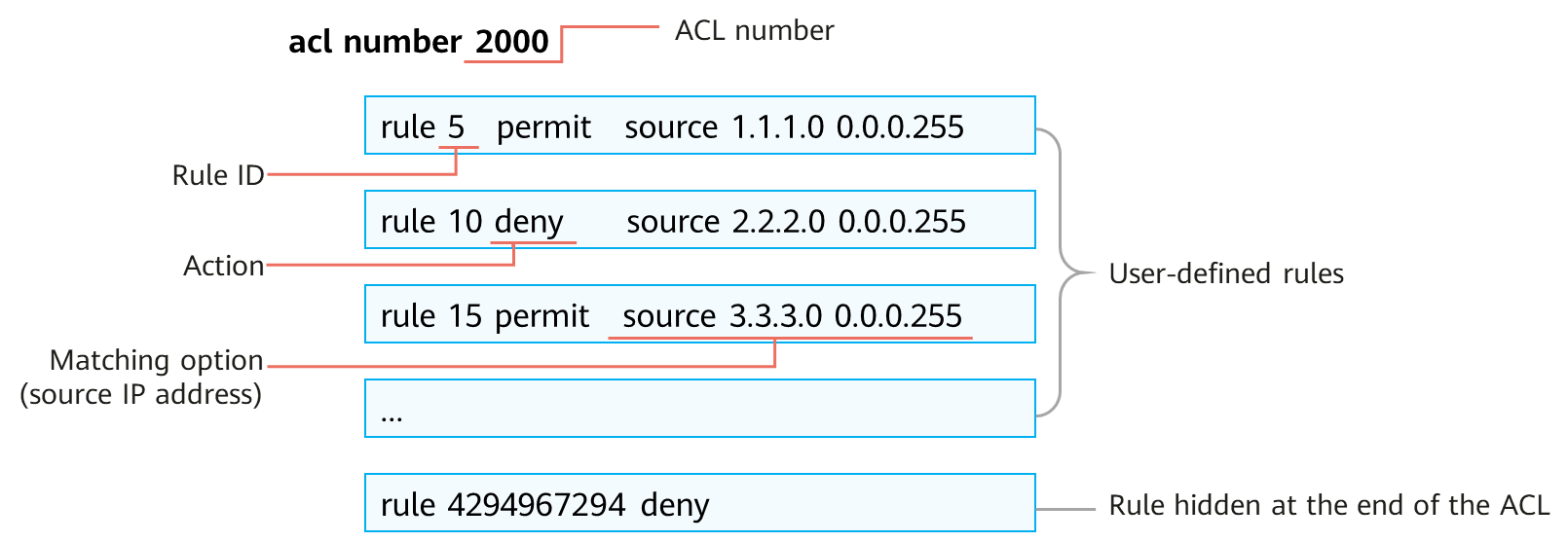
An ACL can match elements such as source and destination IP addresses, source and destination port numbers, and protocol types in IP datagrams. It can also match routes.

In this course, traffic filtering is used to describe ACLs.

## Basic Concepts and Working Mechanism of ACLs

### ACL Composition

An ACL consists of several permit or deny statements. Each statement is a rule of the ACL, and permit or deny in each statement is the action corresponding to the rule.

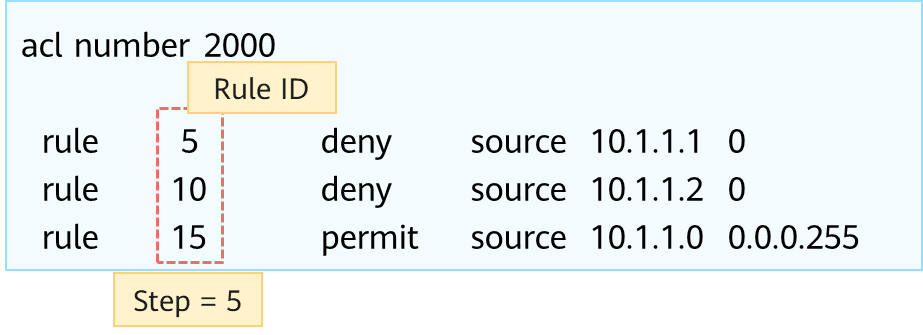


ACL composition

ACL composition:

* ACL number: An ACL is identified by an ACL number. Each ACL needs to allocated an ACL number. The ACL number range varies according to the ACL type, which will be described later.
* Rule: As mentioned above, an ACL consists of several permit/deny statements, and each statement is a rule of the ACL.
* Rule ID: Each ACL rule has an ID, which identifies the rule. Rule IDs can be manually defined or automatically allocated by the system. A rule ID ranges from 0 to 4294967294. All rules are arranged in the ascending order of rule ID.
* Action: Each rule contains a permit or deny action. ACLs are usually used together with other technologies, and the meanings of the permit and deny actions may vary according to scenarios.
  1. For example, if an ACL is used together with traffic filtering technology (that is, the ACL is invoked in traffic filtering), the permit action allows traffic to pass and the deny action rejects traffic.
* Matching option: ACLs support various matching options. In this example, the matching option is a source IP address. The ACL also supports other matching options, such as Layer 2 Ethernet frame header information (including source and destination MAC addresses and Ethernet frame protocol type), Layer 3 packet information (including destination address and protocol type), and Layer 4 packet information (including TCP/UDP port number).

### Rule ID



Rule ID

Rule ID：

Each rule in an ACL has an ID, which identifies the rule. Rule IDs can be manually defined or automatically allocated by the system.

Step：

A step is an increment between neighboring rule IDs automatically allocated by the system. The default step is 5. Setting a step facilitates rule insertion between existing rules of an ACL.

When the system automatically allocates IDs to ACL rules, the increment between neighboring rule IDs is called a step. The default step is 5. Therefore, rule IDs are 5, 10, 15, and so on.

If a rule is manually added to an ACL but no ID is specified, the system allocates to this rule an ID that is greater than the largest rule ID in the ACL and is the smallest integer multiple of the step value.

The step can be changed. For example, if the step is changed to 2, the system automatically renumbers the rule IDs as 2, 4, 6...

Rule ID allocation：

If a rule is added to an empty ACL but no ID is manually specified for the rule, the system allocates a step value (5 for example) as the ID of the rule. If an ACL contains rules with manually specified IDs and a rule with no manually specified ID is added, the system allocates to this rule an ID that is greater than the largest rule ID in the ACL and is the smallest integer multiple of the step value.

What is the function of a step? Why can't rules 1, 2, 3, and 4 be directly used?

First, let's look at a question. How do I add a rule?

We can manually add rule 11 between rules 10 and 15.

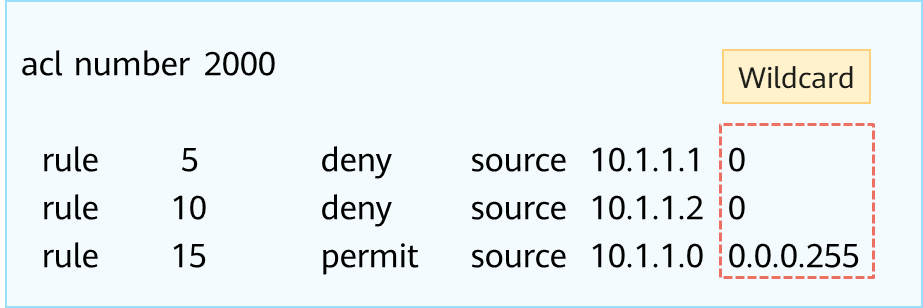
Therefore, setting a step of a certain length facilitates rule insertion between existing rules.

How to add a rule?

Using the follow command:

rule 11 deny source 10.1.1.3 0

### Wildcard (1)



Wildcard

A wildcard is a 32-bit number that indicates which bits in an IP address need to be strictly matched and which bits do not need to be matched.

A wildcard is usually expressed in dotted decimal notation, as a network mask is expressed. However, their meanings are different.

Matching rule:

1. 0: Strict matching
2. 1: Not required

When an IP address is matched, a 32-bit mask is followed. The 32-bit mask is called a wildcard.

A wildcard is also expressed in dotted decimal notation. After the value is converted to a binary number, the value 0 indicates that the equivalent bit must match and the value 1 indicates that the equivalent bit does not matter.

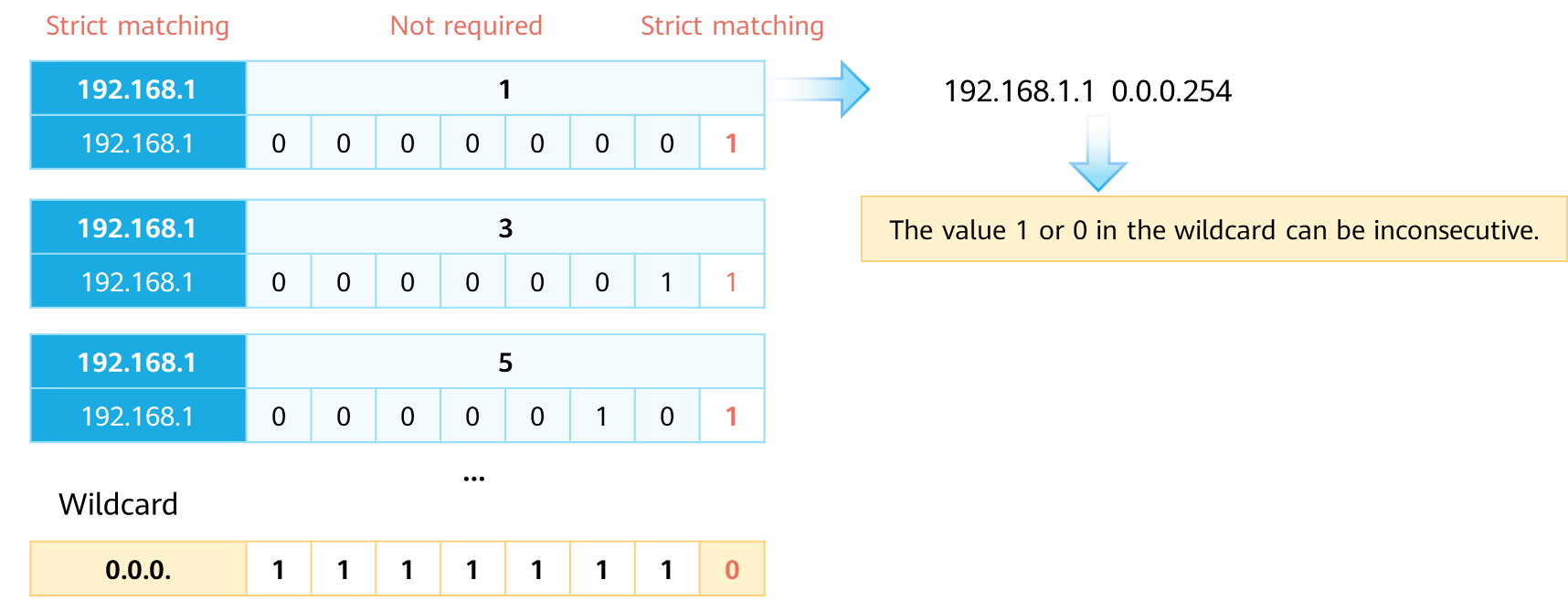
Let's look at two rules:

1. rule 5: denies the packets with the source IP address 10.1.1.1. Because the wildcard comprises all 0s, each bit must be strictly matched. Specifically, the host IP address 10.1.1.1 is matched.
2. rule 15: permits the packets with the source IP address on the network segment 10.1.1.0/24. The wildcard is 0.0.0.11111111, and the last eight bits are 1s, indicating that the bits do not matter. Therefore, the last eight bits of 10.1.1.xxxxxxxx can be any value, and the 10.1.1.0/24 network segment is matched.

For example, if we want to exactly match the network segment address corresponding to 192.168.1.1/24, what is the wildcard?

It can be concluded that the network bits must be strictly matched and the host bits do not matter. Therefore, the wildcard is 0.0.0.255.

### Wildcard (2)



Wildcard (2)

A wildcard can be used to match odd IP addresses in the network segment 192.168.1.0/24, such as 192.168.1.1, 192.168.1.3, and 192.168.1.5.

How do I set the wildcard to match the odd IP addresses in the network segment 192.168.1.0/24?

* First, let's look at the odd IP addresses, such as 192.168.1.1, 192.168.1.5, and 192.168.1.11.
* After the last eight bits are converted into binary numbers, the corresponding addresses are 192.168.1.00000001, 192.168.1.00000101, and 192.168.1.00001011.
* We can see the common points. The seven most significant bits of the last eight bits can be any value, and the least significant bit is fixed to 1. Therefore, the answer is 192.168.1.1 0.0.0.254 (0.0.0.11111110).

In conclusion, 1 or 0 in a wildcard can be inconsecutive.

There are two special wildcards.

* If a wildcard comprising all 0s is used to match an IP address, the address is exactly matched,for example:192.168.1.1 0.0.0.0 = 192.168.1.1 0,Exactly match the IP address 192.168.1.1.
* If a wildcard comprising all 1s is used to match 0.0.0.0, all IP addresses are matched,for example:0.0.0.0 255.255.255 = any,Match All IP addresses.

### ACL Classification and Identification

|  |  |  |
| --- | --- | --- |
| **Category** | **Number Range** | **Description** |
| Basic ACL | 2000 to 2999 | Defines rules based on source IPv4 addresses, fragmentation information, and effective time ranges. |
| Advanced ACL | 3000 to 3999 | Defines rules based on source and destination IPv4 addresses, IPv4 protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and effective time ranges. |
| Layer 2 ACL | 4000 to 4999 | Defines rules based on information in Ethernet frame headers of packets, such as source and destination MAC addresses and Layer 2 protocol types. |
| User-defined ACL | 5000 to 5999 | Defines rules based on packet headers, offsets, character string masks, and user-defined character strings. |
| User ACL | 6000 to 6999 | Defines rules based on source IPv4 addresses or user control list (UCL) groups, destination IPv4 addresses or destination UCL groups, IPv4 protocol types, ICMP types, TCP source/destination port numbers, and UDP source/destination port numbers. |

ACL classification based on ACL rule definition methods

Based on ACL rule definition methods, ACLs can be classified into the following types:

* Basic ACL
* advanced ACL
* Layer 2 ACL
* user-defined ACL
* user ACL

|  |  |
| --- | --- |
| **Category** | **Description** |
| Numbered ACL | Traditional ACL identification method. A numbered ACL is identified by a number. |
| Named ACL | A named ACL is identified by a name. |

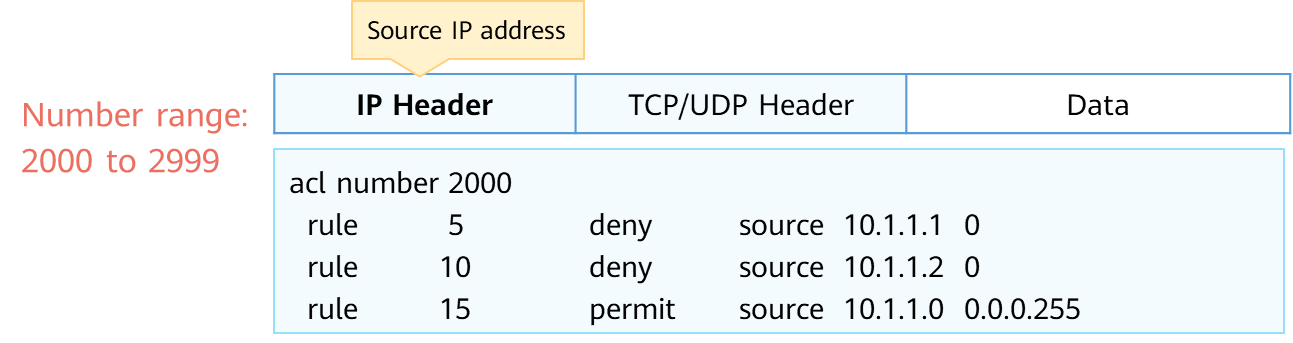
ACL classification based on ACL identification methods

Based on ACL identification methods, ACLs can be classified into the following types:

* Numbered ACL
* Nmed ACL

Note: You can specify a number for an ACL. The ACLs of different types have different number ranges. You can also specify a name for an ACL to help you remember the ACL's purpose. A named ACL consists of a name and number. That is, you can specify an ACL number when you define an ACL name. If you do not specify a number for a named ACL, the system automatically allocates a number to it.

### Basic and Advanced ACLs

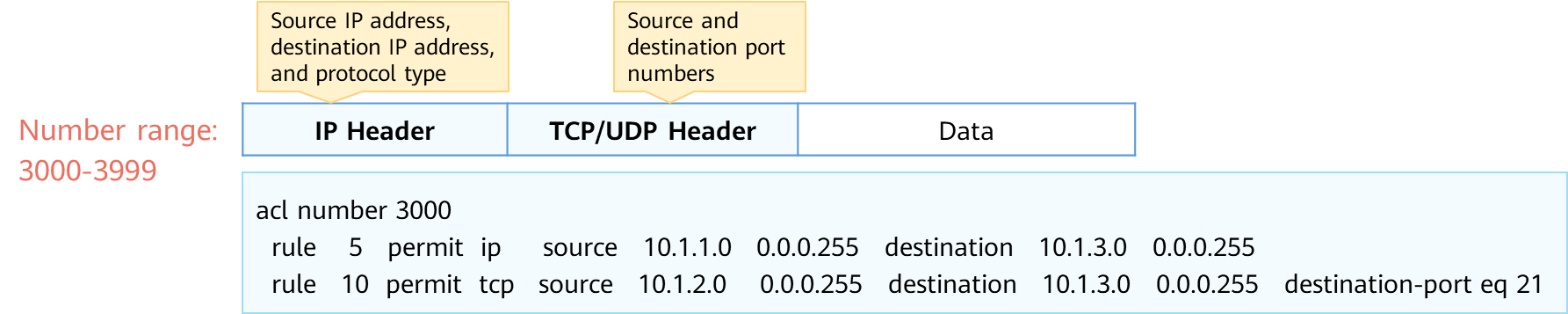


Basic ACL

Basic ACL:

A basic ACL is used to match the source IP address of an IP packet. The number of a basic ACL ranges from 2000 to 2999.

In this example, ACL 2000 is created. This ACL is a basic ACL.

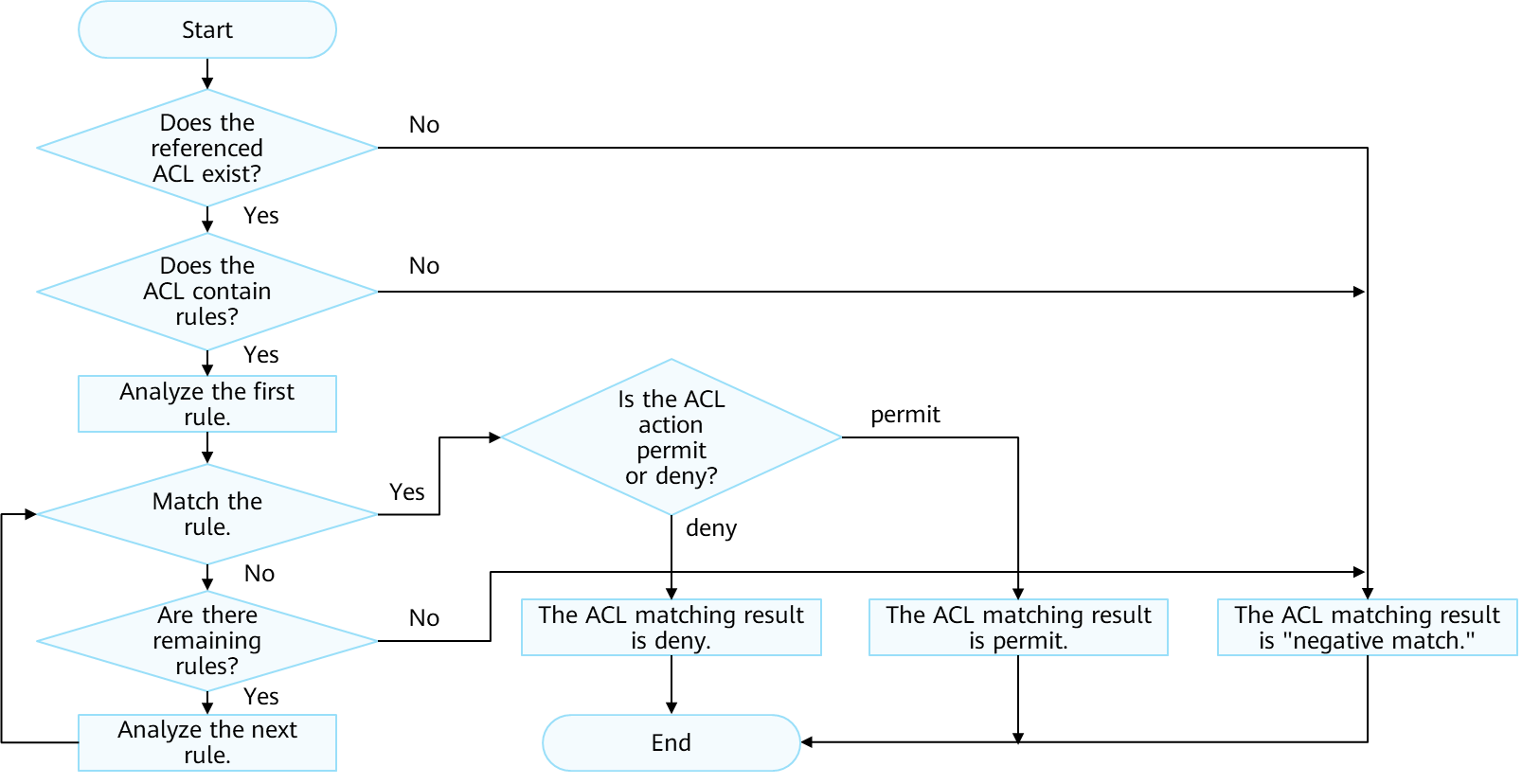


Advanced ACL

Advanced ACL:

An advanced ACL can be matched based on elements such as the source IP address, destination IP address, protocol type, and TCP or UDP source and destination port numbers in an IP packet. A basic ACL can be regarded as a subset of an advanced ACL. Compared with a basic ACL, an advanced ACL defines more accurate, complex, and flexible rules.

### ACL Matching Mechanism



ACL Matching Mechanism

The ACL matching mechanism is as follows:

* After receiving a packet, the device configured with an ACL matches the packet against ACL rules one by one. If the packet does not match any ACL rule, the device attempts to match the packet against the next ACL rule.
* If the packet matches an ACL rule, the device performs the action defined in the rule and stops the matching.

Matching process: The device checks whether an ACL is configured.

* If no ACL is configured, the device returns the result "negative match."
* If an ACL is configured, the device checks whether the ACL contains rules.

1. If the ACL does not contain rules, the device returns the result "negative match."
2. If the ACL contains rules, the device matches the packet against the rules in ascending order of rule ID.
3. If the packet matches a permit rule, the device stops matching and returns the result "positive match (permit)."
4. If the packet matches a deny rule, the device stops matching and returns the result "positive match (deny)."
5. If the packet does not match any rule in the ACL, the device returns the result "negative match."

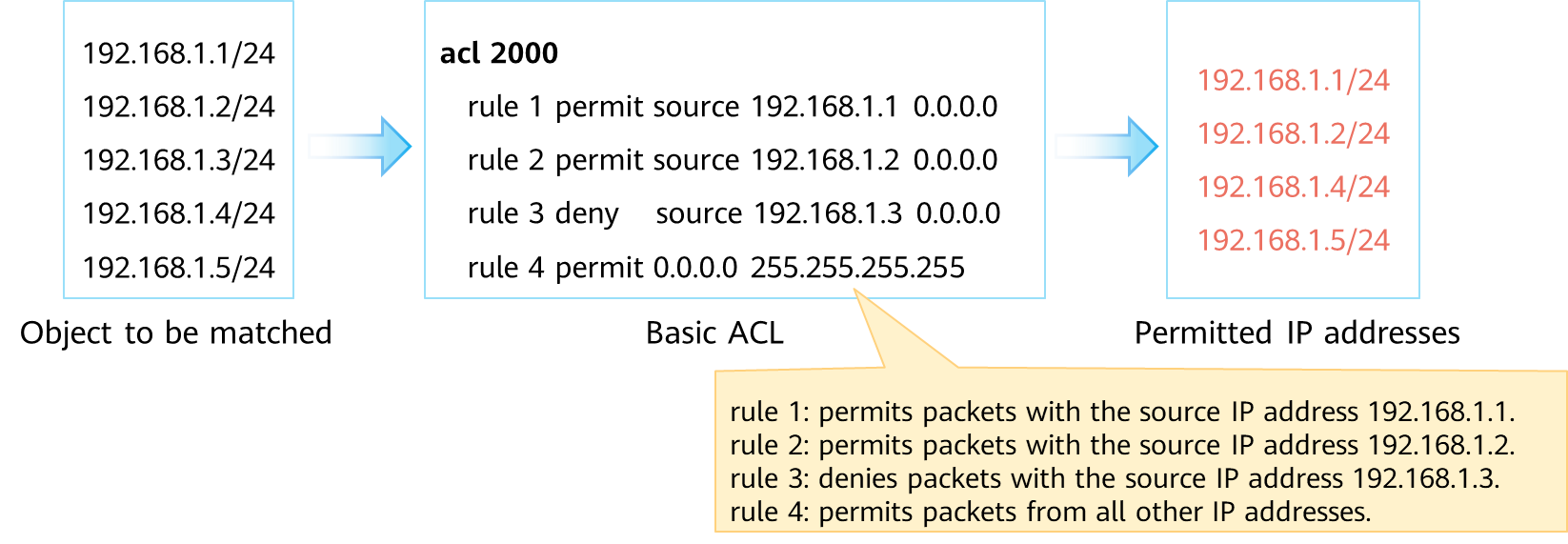
The ACL matching results include "positive match" and "negative match."

* Positive match: Packets match a rule in an ACL. The result is "positive match" regardless of whether packets match a permit or deny rule in an ACL.
* Negative match: No ACL exists, the ACL does not contain rules, or packets do not match any rule in an ACL.

Matching principle: The matching stops once a rule is matched.

### ACL Matching Order and Result

Configuration order (config mode):The system matches packets against ACL rules in ascending order of rule ID. That is, the rule with the smallest ID is processed first.



ACL Matching Order and Result

An ACL can consist of multiple deny or permit statements. Each statement describes a rule. Rules may overlap or conflict. Therefore, the ACL matching order is very important.

Huawei devices support two matching orders: automatic order (auto) and configuration order (config). The default matching order is config.

* auto: The system arranges rules according to the precision of the rules ("depth first" principle), and matches packets against the rules in descending order of precision. ––This is complicated and is not detailed here. If you are interested in it, you can view related materials after class.
* config: The system matches packets against ACL rules in ascending order of rule ID. That is, the rule with the smallest ID is processed first. ––This is the matching order mentioned above.

1. If another rule is added, the rule is added to the corresponding position, and packets are still matched in ascending order.

Matching result:

First, let's understand the meaning of ACL 2000.

* rule 1: permits packets with the source IP address 192.168.1.1.
* rule 2: permits packets with the source IP address 192.168.1.2.
* rule 3: denies packets with the source IP address 192.168.1.3.
* rule 4: permits packets from all other IP addresses.

When packets with the source IP address 192.168.1.3 pass through the device configured with the ACL:

* The device matches the packets against rule 1. The matching result is "negative match."
* The device continues to match the packets against rule 2. The matching result is still "negative match."
* The device continues to match the packets against rule 3. The matching result is "positive match," and the action is deny.

Note: ACLs are usually used together with other technologies, and the meanings of the permit and deny actions may vary according to scenarios.For example, if an ACL is used together with traffic filtering technology (that is, the ACL is invoked in traffic filtering), the permit action allows traffic to pass and the deny action rejects traffic.

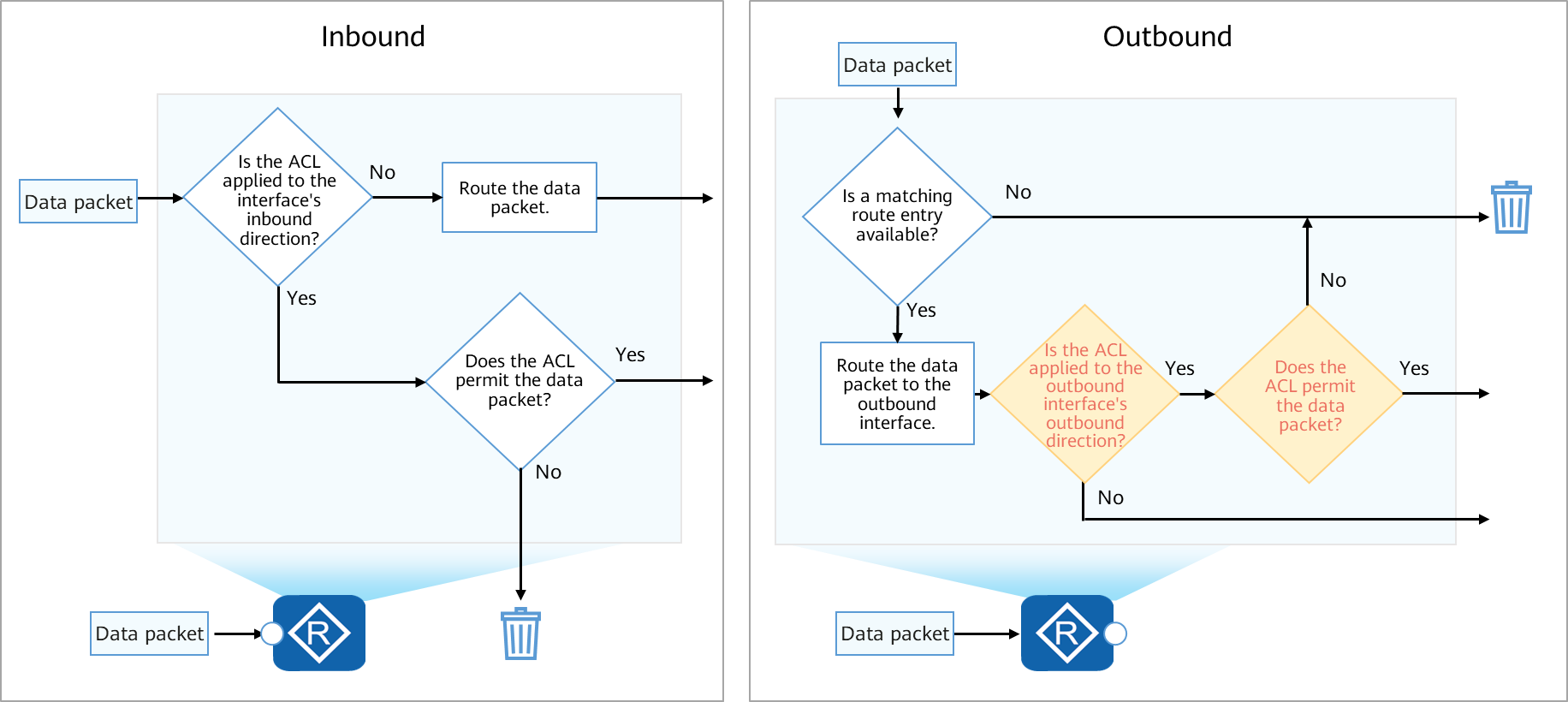
### ACL Matching Position



ACL Matching Position

Position 1:Configure an ACL on the interface.To enable the ACL to take effect for the data packet shown in the figure,apply the ACL to the inbound direction.

Position 2:Configure an ACL on the interface.To enable the ACL to take effect for the data packet shown in the figure,apply the ACL to the outbound direction.



Inbound and Outbound Directions

## Basic Configurations and Applications of ACLs

### Basic Configuration Commands of Basic ACLs

* Create a basic ACL.

[Huawei] **acl** [ **number** ] *acl-number* [ **match-order config** ]

Create a numbered basic ACL and enter its view.

1. *acl-number*: specifies the number of an ACL.
2. **match-order config**: indicates the matching order of ACL rules. config indicates the configuration order.

* Configure a rule for the basic ACL.

[Huawei-acl-basic-2000] **rule** [ *rule-id* ] { **deny | permit** } [ **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* ]

In the basic ACL view, you can run this command to configure a rule for the basic ACL.

1. *rule-id*: specifies the ID of an ACL rule.
2. **deny**: denies the packets that match the rule.
3. **permit**: permits the packets that match the rule.
4. **source** { *source-address source-wildcard* | **any** }: specifies the source IP address of packets that match the ACL rule. If no source address is specified, packets with any source addresses are matched.
5. source-address: specifies the source IP address of packets.
6. source-wildcard: specifies the wildcard of the source IP address.
7. any: indicates any source IP address of packets. That is, the value of source-address is 0.0.0.0 or the value of source-wildcard is 255.255.255.255.
8. **time-range** *time-name*: specifies a time range in which the ACL rule takes effect. time-name specifies the name of a time range. If no time range is specified, the ACL rule is always valid.

### Case: Use a Basic ACL to Filter Data Traffic

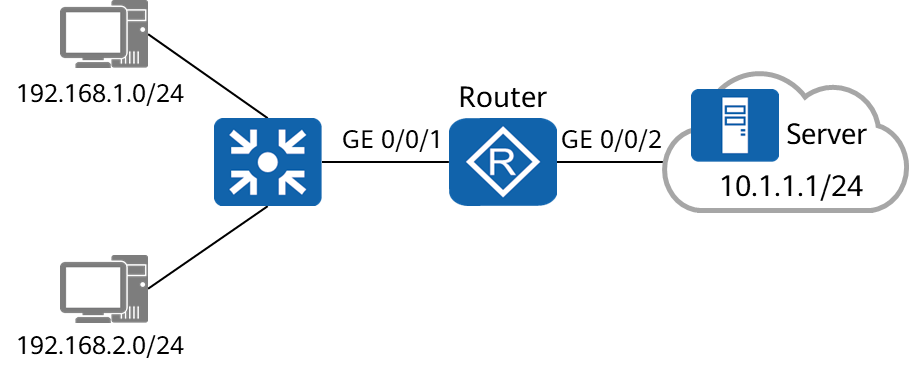


Diagram of Case

Requirements:

To prevent the user host on the network segment 192.168.1.0/24 from accessing the network where the server resides, configure a basic ACL on the router. After the configuration is complete, the ACL filters out the data packets whose source IP addresses are on the network segment 192.168.1.0/24 and permits other data packets.

Configuration roadmap:

Configure a basic ACL and traffic filtering to filter packets from a specified network segment.

Procedure:

* Configure IP addresses and routes on the router.
* Create ACL 2000 and configure ACL rules to deny packets from the network segment 192.168.1.0/24 and permit packets from other network segments.
* Configure traffic filtering.

Note:

* The **traffic-filter** command applies an ACL to an interface to filter packets on the interface.
* Command format: **traffic-filter** { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }

1. **inbound**: configures ACL-based packet filtering in the inbound direction of an interface.
2. **outbound**: configures ACL-based packet filtering in the outbound direction of an interface.
3. **acl**: filters packets based on an IPv4 ACL.

Step of configuration：

Step 1 Configure IP addresses and routes on the router.

Step 2 Create a basic ACL on the router to prevent the network segment 192.168.1.0/24 from accessing the network where the server resides.

[Router] **acl** 2000

[Router-acl-basic-2000] **rule deny source** 192.168.1.0 0.0.0.255

[Router-acl-basic-2000] **rule permit source any**

Step 3 Configure traffic filtering in the inbound direction of GE 0/0/1.

[Router] interface GigabitEthernet 0/0/1

[Router-GigabitEthernet0/0/1] **traffic-filter inbound acl 2000**

[Router-GigabitEthernet0/0/1] quit

### Basic Configuration Commands of Advanced ACLs

* Create an advanced ACL.

[Huawei] **acl** [ **number** ] *acl-number* [ **match-order config** ]

Create a numbered advanced ACL and enter its view.

1. acl-number: specifies the number of an ACL.
2. match-order config: indicates the matching order of ACL rules. config indicates the configuration order.

[Huawei] **acl name** *acl-name* { **advance** | *acl-number* } [ **match-order config** ]

Create a named advanced ACL and enter its view.

1. acl-name: specifies the name of an ACL.
2. **advance**: indicates an advanced ACL.

* Configure a rule for the advanced ACL.

You can configure advanced ACL rules according to the protocol types of IP packets. The parameters vary according to the protocol types.

When the protocol type is IP, the command format is:

**rule** [ *rule-id* ] { **deny** | **permit** } **ip** [ **destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] ] ]

In the advanced ACL view, you can run this command to configure a rule for the advanced ACL.

1. **ip**: indicates that the protocol type is IP.
2. **destination** { *destination-address destination-wildcard* | any }: specifies the destination IP address of packets that match the ACL rule. If no destination address is specified, packets with any destination addresses are matched.
3. **dscp** *dscp*: specifies the differentiated services code point (DSCP) of packets that match the ACL rule. The value ranges from 0 to 63.
4. **tos** *tos*: specifies the ToS of packets that match the ACL rule. The value ranges from 0 to 15.
5. **precedence** *precedence*: specifies the precedence of packets that match the ACL rule. The value ranges from 0 to 7.

When the protocol type is TCP, the command format is:

**rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **tcp** } [ **destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** port | **gt** port | **lt** port | **range** port-start port-end } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** port | **gt** port | **lt** port | **range** port-start port-end } **| tcp-flag** { **ack** | **fin** | **syn** } \* | **time-range** time-name ] \*

In the advanced ACL view, you can run this command to configure a rule for the advanced ACL.

1. **tcp**: indicates that the protocol type is TCP. You can set protocol-number to 6 to indicate TCP.
2. **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }: specifies the TCP destination port number of packets that match the ACL rule. The value is valid only when the protocol type is TCP. If no destination port number is specified, packets with any TCP destination port numbers are matched.
3. **eq** *port*: equal to the destination port number
4. **gt** *port*: greater than the destination port number
5. **lt** *port*: less than the destination port number
6. **range** *port-start port-end*: specifies a source port number range.
7. **tcp-flag**: indicates the SYN Flag in the TCP packet header.

### Case: Use Advanced ACLs to Prevent User Hosts on Different Network Segments from Communicating

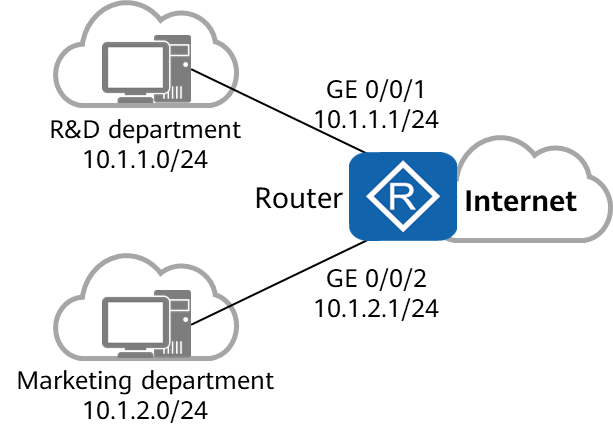


Diagram of case

Requirements:

The departments of a company are connected through the router. To facilitate network management, the administrator allocates IP addresses of different network segments to the R&D and marketing departments.

The company requires that the router prevent the user hosts on different network segments from communicating to ensure information security.

Configuration roadmap:

Configure an advanced ACL and traffic filtering to filter the packets exchanged between the R&D and marketing departments.

Procedure:

* Configure IP addresses and routes on the router.
* Create ACL 3001 and configure rules for the ACL to deny packets from the R&D department to the marketing department.
* Create ACL 3002 and configure rules for the ACL to deny packets from the marketing department to the R&D department.
* Configure traffic filtering in the inbound direction of GE 0/0/1 and GE 0/0/2.

Note:

* The **traffic-filter** command applies an ACL to an interface to filter packets on the interface.
* Command format: **traffic-filter** { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }

1. **inbound**: configures ACL-based packet filtering in the inbound direction of an interface.
2. **outbound**: configures ACL-based packet filtering in the outbound direction of an interface.
3. **acl**: filters packets based on an IPv4 ACL.

Step of configuration：

Step 1 Configure IP addresses and routes on the router.

Step 2 Create ACL 3001 and configure rules for the ACL to deny packets from the R&D department to the marketing department.

[Router] **acl** 3001

[Router-acl-adv-3001] **rule deny ip source** 10.1.1.0 0.0.0.255 **destination** 10.1.2.0 0.0.0.255

[Router-acl-adv-3001] quit

Step3 Create ACL 3002 and configure rules for the ACL to deny packets from the marketing department to the R&D department.

[Router] **acl** 3002

[Router-acl-adv-3002] **rule deny ip source** 10.1.2.0 0.0.0.255 **destination** 10.1.1.0 0.0.0.255

[Router-acl-adv-3002] quit

Step4 Configure traffic filtering in the inbound direction of GE 0/0/1 and GE 0/0/2.

[Router] interface GigabitEthernet 0/0/1

[Router-GigabitEthernet0/0/1] **traffic-filter inbound acl 3001**

[Router-GigabitEthernet0/0/1] quit

[Router] interface GigabitEthernet 0/0/2

[Router-GigabitEthernet0/0/2] **traffic-filter inbound acl 3002**

[Router-GigabitEthernet0/0/2] quit

## Summary

ACL is a widely used network technology. Its principle is as follows: packets are matched against configured ACL rules and actions are taken on the packets as configured in the ACL rules. The matching rules and actions are configured based on network requirements. Due to the variety of matching rules and actions, ACLs can implement a lot of functions.

ACLs are often used with other technologies, such as firewall, routing policy, QoS, and traffic filtering.

## Quiz

1. (Single) Which one of the following rules is a valid basic ACL rule? ( )
2. rule permit ip
3. rule deny ip
4. rule permit source any
5. rule deny tcp source any
6. (Single) Which of the following ACL rules can the traffic destined for 192.168.1.1/24 be permitted? ( )
7. rule permit source 192.168.1.1 0.0.0.255
8. rule permit source 192.168.1.0 0.0.0.254
9. rule permit source 192.168.0.0 0.0.0.255
10. rule deny source any
11. (Single) Which of the following cannot be controlled by ACL 3001? ( )
12. Destination address
13. Source address
14. Destination port number
15. Packet length
16. (Multiple) What are the applications of ACLs? ( )
17. Provide means of controlling communication traffic
18. Is a basic means of providing network security access
19. Called in QoS
20. Matches routes.
21. (True or False) The default step for configuring an ACL is 5. The step can be changed. ( )
22. True
23. False
24. (True or False) The configuration commands of ACL 2001 are as follows:

Rule 5 permit source 192.168.1.1 0.0.0.0

Rule 10 deny source 192.168.1.1 0.0.0.0

Then, the traffic with the destination address 192.168.1.1 is permitted. ( )

1. True
2. False
3. Which parameters can you use to define advanced ACL rules?