ACL Principles and Configuration

1 ACL Principles and Configuration

1.1 ACL Overview

1.1.1 Network Security and QoS

1.1.1.1 Key Issues

- Unauthorized access to enterprise key servers.
- Confidential information leakage.
- Internet viruses threatening intranet security.
- Random service traffic occupying bandwidth.
- Lowered user experience due to compromised QoS for delay-sensitive services.

1.1.1.2 Solution: Traffic Filtering

1.1.1.2.1 Access Control List (ACL) Overview

1.1.1.2.1.1 What is an ACL?

> An ACL is a set of sequential rules composed of permit or deny statements that matches and distinguishes packets based on predefined criteria.

1.1.1.2.1.2 Matching Criteria

- Source IP address
- Destination IP address
- Protocol type
- Source port number (TCP/UDP)
- Destination port number (TCP/UDP)

1.1.1.2.1.3 Applications of ACLs

Application	Description
Traffic Filter	Filters traffic as part of network security measures.
NAT	Used in Network Address Translation configurations.
Routing Policy	Influences route selection processes.
Firewall Policy	Part of defining firewall behaviors.
QoS	Improves Quality of Service by prioritizing traffic.

1.1.1.2.1.4 Importance of ACLs

> ACLs are crucial for identifying and controlling packets to manage network access behaviors, prevent attacks, and improve bandwidth

> utilization.

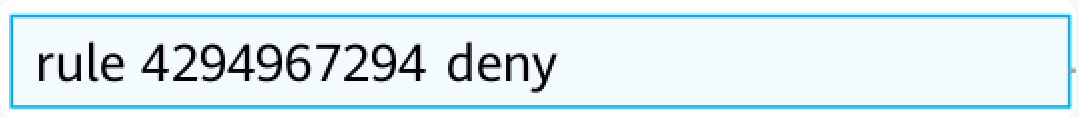
1.2 Basic Concepts and Working Mechanism of ACLs

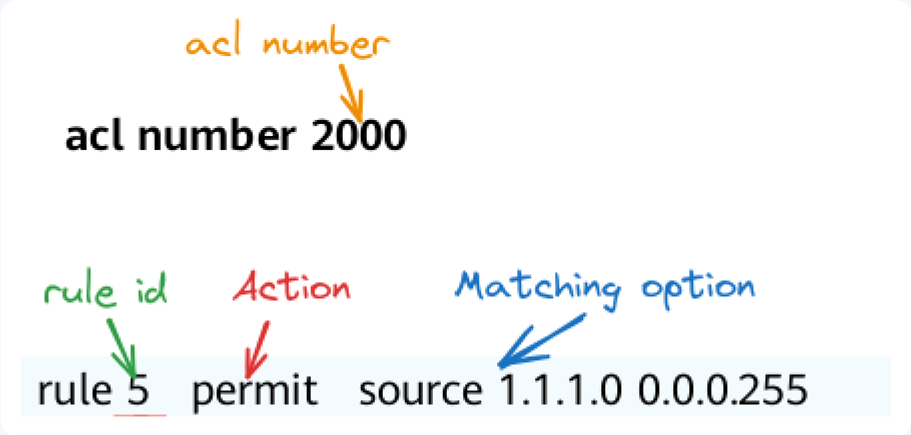
1.2.1 Composition of ACLs

- **ACL Number**: Unique identifier for each ACL.
- **Rule ID**: Identifier for each rule within an ACL; ranges from 0 to 4294967294.
- **Action**: Specifies whether to "permit" or "deny" matching packets.
- **Matching Option**: Criteria used to match packets (e.g., source IP address).

> Rule IDs can be **manually** defined or **automatically** (The default step is 5 for increment between rules Therefore, rule IDs are 5, 10, 15, and so on.) allocated by the system.

> When a new rule is manually defined added without a specified number, the computer assigns the next-highest number following an adjustable stepwise pattern, renumbering all rules accordingly if the step size changes.

> **Rule hidden at the end of the ACL:**
>
> 
>
> ```
> rule 4294967294 deny
> ```
>
> It acts as a last final option to deny access when all other rules have been checked and don't grant permission.

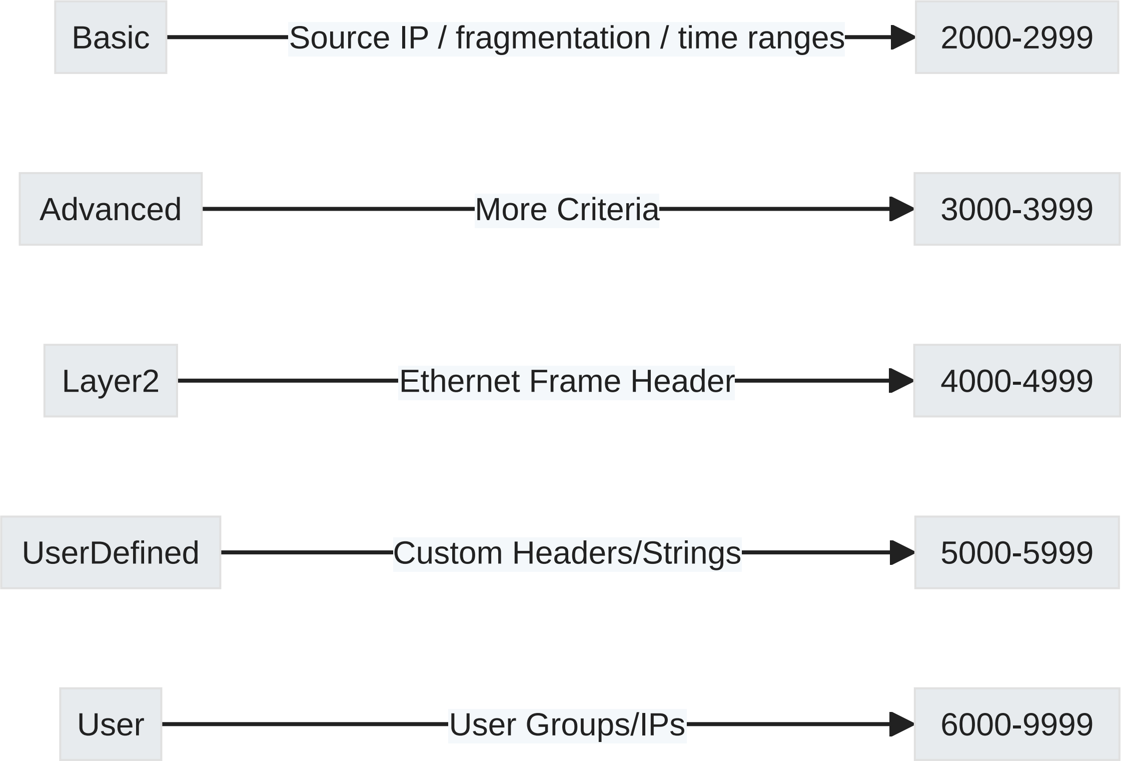


```
acl number 2000

rule 5   permit   source 1.1.1.0 0.0.0.255
```

1.2.2 Classification of ACLs

Based on how rules are defined, we have different types of ACLs:



Basic → Source IP / fragmentation / time ranges → 2000-2999

Advanced → More Criteria → 3000-3999

Layer2 → Ethernet Frame Header → 4000-4999

UserDefined → Custom Headers/Strings → 5000-5999

User → User Groups/IPs → 6000-9999

> **More Criteria:**
>
> - source and destination IPv4 addresses.
> - IPv4 protocol types.
> - ICMP types.
> - TCP source/destination port numbers.

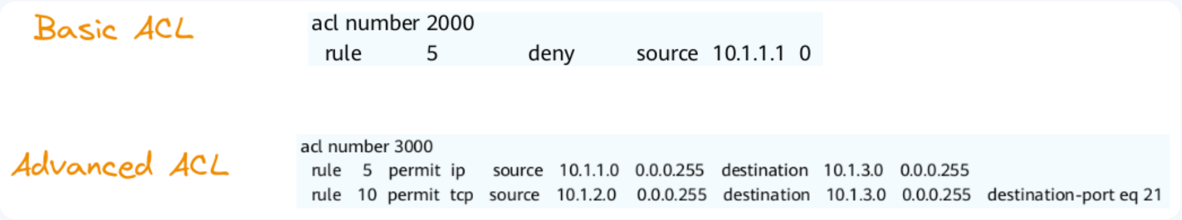
- UDP source/destination port numbers.
- effective time ranges.

Ethernet frame headers:

- source and destination MAC addresses.
- Layer 2 protocol types.

Custom Headers/Strings:

- packet headers.
- offsets.
- character string masks.
- user-defined character strings.



```
acl number 2000
 rule    5       deny      source  10.1.1.1  0
```

```
acl number 3000
 rule   5  permit  ip    source   10.1.1.0   0.0.0.255   destination   10.1.3.0   0.0.0.255
 rule  10  permit  tcp   source   10.1.2.0   0.0.0.255   destination   10.1.3.0   0.0.0.255   destination-port eq 21
```

1.2.2.1 Identification Methods

There are two ways to identify an ACL: by number or by name. Named ACLs are easier to remember and manage.

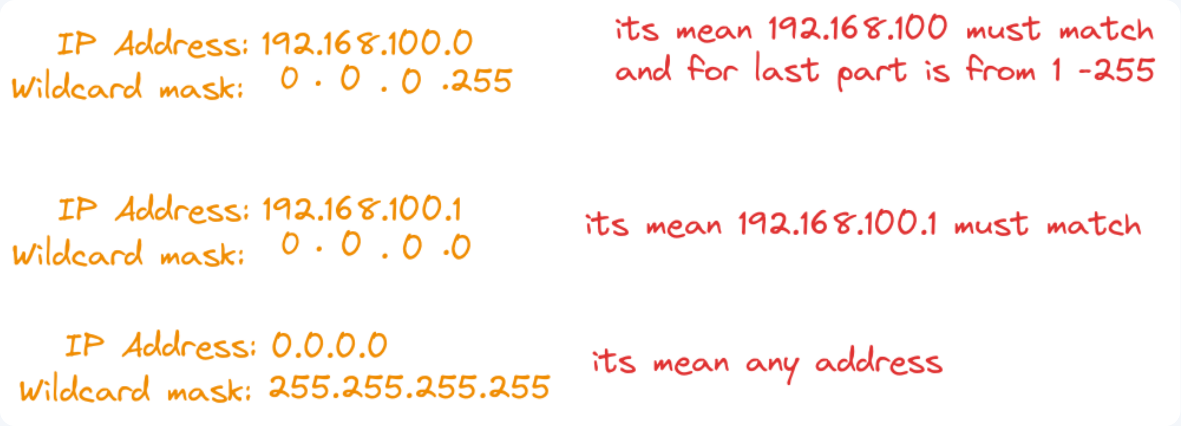
1.2.3 Matching Rules in ACLs

1.2.3.1 Wildcards

Wildcards determine which bits in an IP address must match exactly (`0`) and which bits can vary (`1`).

> A wildcard is a 32-bit number.

> A wildcard is usually expressed in dotted decimal notation.



IP Address: 192.168.100.0
Wildcard mask: 0 . 0 . 0 .255

its mean 192.168.100 must match
and for last part is from 1 -255

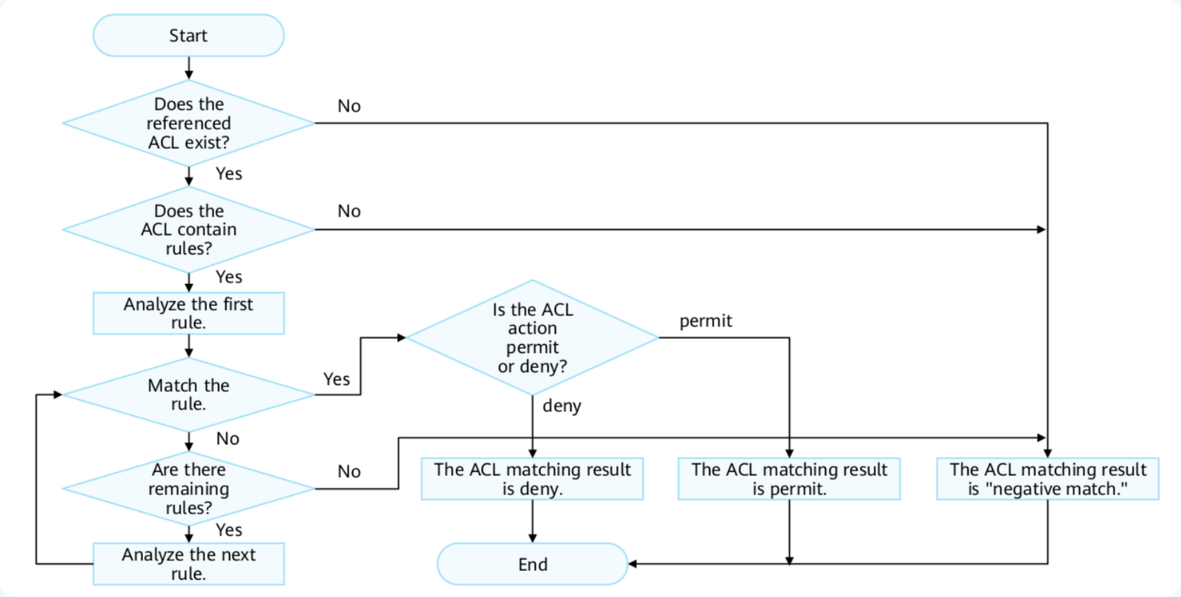
IP Address: 192.168.100.1
Wildcard mask: 0 . 0 . 0 .0

its mean 192.168.100.1 must match

IP Address: 0.0.0.0
Wildcard mask: 255.255.255.255

its mean any address

1.2.3.2 Matching Order & Result


Start
Does the referenced ACL exist?
No
Yes
Does the ACL contain rules?
No
Yes
Analyze the first rule.
Is the ACL action permit or deny?
permit
Yes
Match the rule.
deny
No
Are there remaining rules?
No
The ACL matching result is deny.
The ACL matching result is permit.
The ACL matching result is "negative match."
Yes
Analyze the next rule.
End

- ACL matching checks packets against rules sequentially.

- Stops at first match, performs action (permit/deny), no further checks.
- No ACL or no rules results in negative match.
- Matches are either positive (permit or deny) or negative.

ACL rules are processed in ascending order of their Rule IDs until a match is found.

Rule ID	Action	Source	Description
1	permit	192.168.1.1/32	Permits only from 192.168.1.1
2	permit	192.168.1.2/32	Permits only from 192.168.1.2
3	deny	192.168.1.3/32	Denies from 192.168.1.3

> The first matching rule determines the action taken; subsequent rules are ignored.

Note

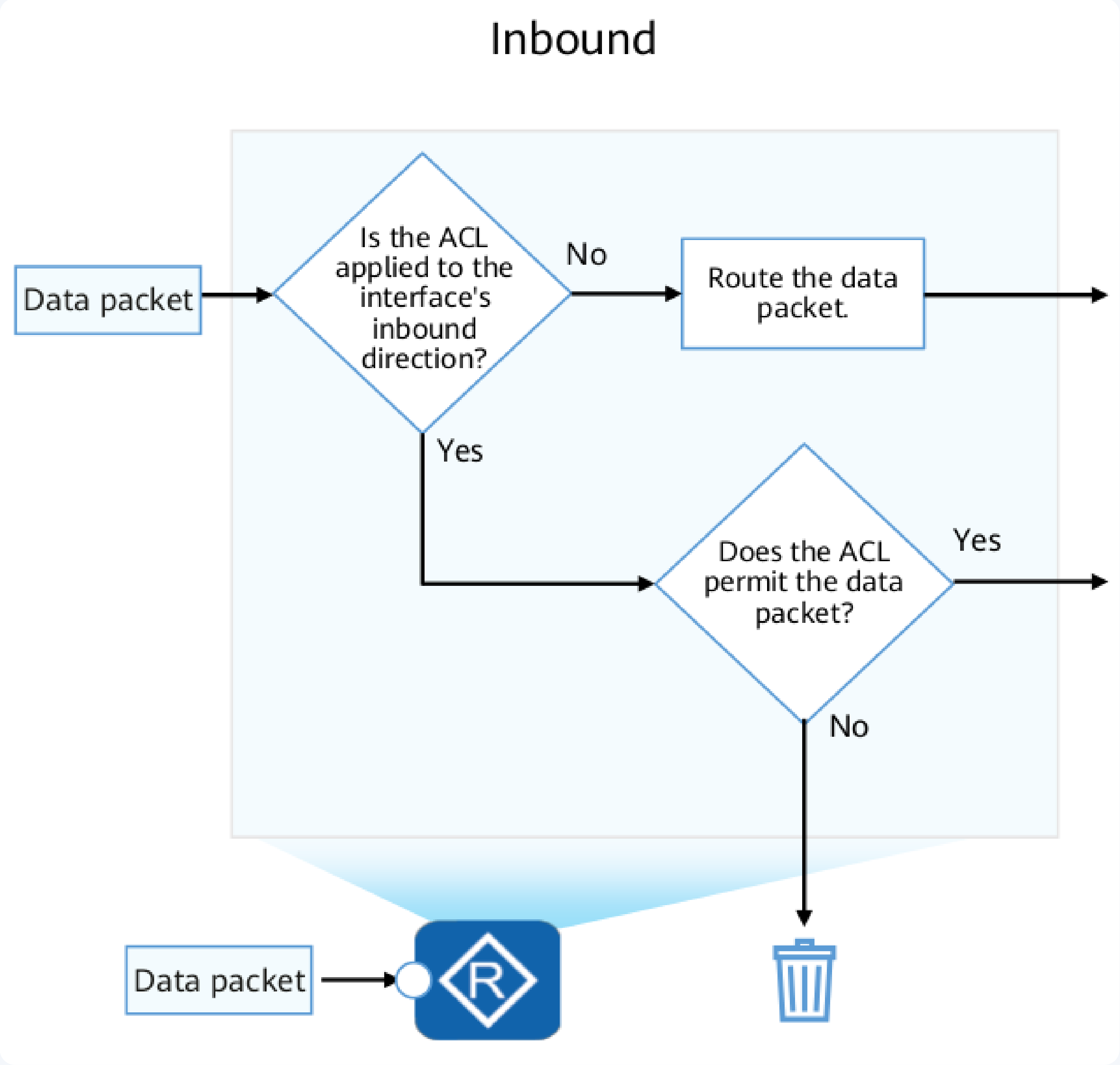
Huawei devices have two ways to decide which rule gets applied first when filtering network traffic:

- **auto:** automatically prioritizes network traffic rules by placing more specific instructions higher on the list for accurate traffic management.
- **config:** The device checks network traffic against the rules starting from the one with the lowest ID number and moving upwards. By default, this is how rules are matched.

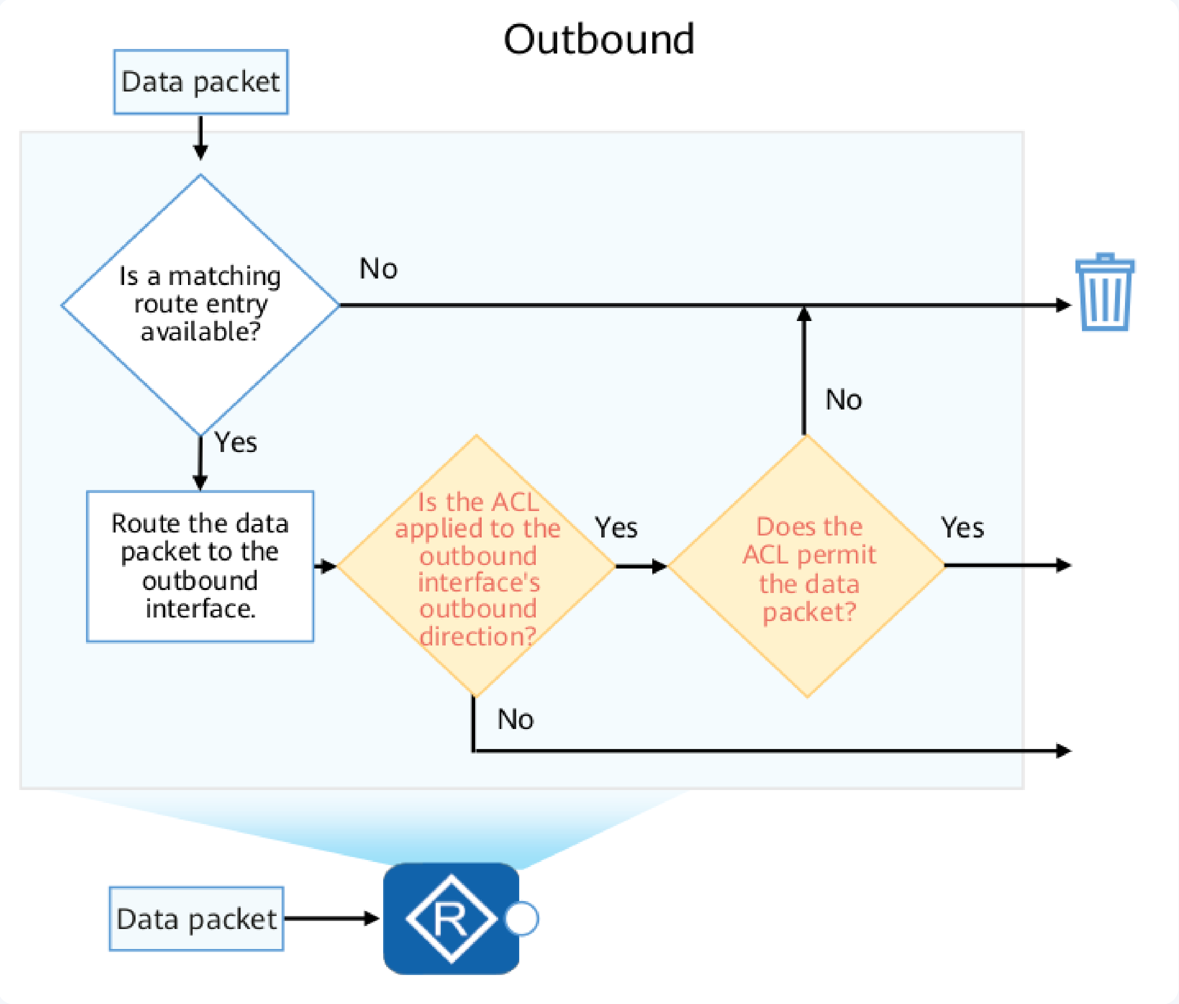
1.2.4 Applying ACLs

1.2.4.1 Directionality

Inbound interface:


Inbound
Data packet
Is the ACL applied to the interface's inbound direction?
No
Route the data packet.
Yes
Does the ACL permit the data packet?
Yes
No
Data packet
R

Outbound interface:


Outbound
Data packet
Is a matching route entry available?
No
Yes
Route the data packet to the outbound interface.
Is the ACL applied to the outbound interface's outbound direction?
Yes
No
Does the ACL permit the data packet?
No
Yes
Data packet
R

1.3 Basic Configurations and Applications of ACLs

1.3.1 Creating a Basic ACL

```
acl number <acl-number> <match-order config>
```

- `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.

  - `sequential` : Rules are evaluated in the order they were entered.

```
acl name <acl-name> <basic>||<acl-number> <match-order config>
```

- `<acl-name>` : Name of the ACL.
- `basic` : Specifies a basic ACL type.
-   - `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.
  - `sequential` : Rules are evaluated in the order they were entered.

1.3.2 Configuring Basic ACL Rules

```
rule <rule-id> <action> source <source-address> <source-wildcard>||any || time-range <time-name>
```

- `<rule-id>` : Optional rule identifier.

> ranges from 0 to 4294967294.

- `<action>` :
  - `deny` : Blocks matching packets.
  - `permit` : Allows matching packets.
- `<source-address>` `<source-wildcard>` : Source IP address and wildcard mask.
- `any` : Matches any source IP address.

- `<time-name>` : Time range name for rule applicability.

1.3.3 Apply acl into interface

```markdown
traffic-filter <interface-bound> acl <acl-option>

```

- `<interface-bound>` :
  - **inbound:** configures ACL-based packet filtering in the inbound direction of an interface.
  - **outbound:** configures ACL-based packet filtering in the outbound direction of an interface.
- `<acl-option>` :
  - **acl-number**
  - **name acl-name**

1.3.4 Creating an Advanced ACL

```markdown
acl number <acl-number> <match-order config>
```

- `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.
  - `sequential` : Rules are evaluated in the order they were entered.

```markdown
```

```
acl name <acl-name> <advance>||<acl-number> <match-order config>
```

- `<acl-name>` : Name of the ACL.
- `basic` : Specifies a basic ACL type.
-
  - `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.
  - `sequential` : Rules are evaluated in the order they were entered.

1.3.5 Configuring Advanced ACL Rules

```markdown
rule <rule-id> <action> ip destination <destination-address> <destination-wildcard>||any source <source-address> <source-wildcard>||any || time-range <time-name>
|| dscp <dscp> || tos <tos> || precedence <precedence>
```

- `<rule-id>` : Optional rule identifier.

> ranges from 0 to 4294967294.

- `<action>` :
  - `deny` : Blocks matching packets.
  - `permit` : Allows matching packets.
- **ip:** indicates that the protocol type is IP.
- `<source-address>` `<source-wildcard>` : Source IP address and wildcard mask.
- `any` : Matches any source IP address.

- `<time-name>` : Time range name for rule applicability.
- `<dscp>` : Sets a priority label (0-63) for matched packets.
- `<tos>` : Sets a type of service label (0-15) for matched packets.
- `<precedence>` : Assigns a priority rank (0-7) for matched packets.

```
rule <rule-id> <action> <protocol> 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> } || time-range <time-name> || tcp-flag <flag>
```

- `<rule-id>` : Optional rule identifier.

> ranges from 0 to 4294967294.

- `<action>` :
  - `deny` : Blocks matching packets.
  - `permit` : Allows matching packets.
- **tcp:** indicates that the protocol type is TCP. You can set protocol-number to 6 to indicate TCP.
- `<source-address>` `<source-wildcard>` : Source IP address and wildcard mask.
- `any` : Matches any source IP address.
- **eq** `<port>` : equal to the destination port number
- **gt** `<port>` : greater than the destination port number
- **lt** `<port>` : less than the destination port number
- **range** `<port-start port-end>` : specifies a source port number range.
- `<time-name>` : Time range name for rule applicability.

- `<flag>:` indicates the SYN Flag in the TCP packet header.