



Access Control Lists (ACLs) User Guide

Version 22.7.1, 25 July 2022

| Registered Address | Support | Sales |
|---|--|--|
| 26, Kingston Terrace, Princeton, New Jersey 08540, United States | | |
| | | +91 80 4850 5445 |
| http://www.rtbrick.com | support@rtbrick.com | sales@rtbrick.com |

©Copyright 2022 RtBrick, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos and service marks ("Marks") displayed in this documentation are the property of RtBrick in the United States and other countries. Use of the Marks are subject to RtBrick's Term of Use Policy, available at <https://www.rtbrick.com/privacy>. Use of marks belonging to other parties is for informational purposes only.

Table of Contents

| | |
|---|----|
| 1. Introduction | 3 |
| 1.1. ACL Use Cases | 3 |
| 1.2. ACL Components and Processing | 3 |
| 1.3. Prefix Lists | 3 |
| 1.4. Supported Platforms | 4 |
| 2. Configuring Access Control Lists | 5 |
| 2.1. Configuration Hierarchy | 5 |
| 2.2. Configuration Syntax and Commands | 5 |
| 2.2.1. Configuring ACLs | 5 |
| 2.2.1.1. Configuring ACL Match Criteria | 6 |
| 2.2.1.2. Configuring ACL Actions | 11 |
| Configuring Prefix Lists | 13 |
| Configuring IPv4/IPv6 Prefix List for ACL and Multifield Classifier | 13 |
| 3. Operational Commands | 14 |
| 3.1. ACL Show and Statistics Commands | 14 |

1. Introduction

1.1. ACL Use Cases

In RBFS, Access Control Lists (ACL) serve multiple purposes:

- Provide security by traffic filtering. This applies to both host and transit traffic. ACLs for traffic filtering are user-defined by configuration.
- Redirecting control traffic to the CPU. Such protocol ACLs, also referred to as trap rules, are automatically created by the respective protocol, and do not need to be configured.
- Classifying traffic for differentiated QoS treatment. This is a special form of ACLs referred to as multi-field (MF) classifiers. For MF classifiers, please refer to the HQoS Configuration Guide.

1.2. ACL Components and Processing

User-defined ACLs consists of rules and ordinals. In case of multiple matching ACL rules, you can use priorities to define the result of the ACL.

- Rules - A rule is a named ACL entry that typically contains one or multiple match criteria and an action.
- Ordinals - An ordinal is solely a numbered configuration object. A rule can consist of multiple ordinals. Ordinals help to structure the configuration. In RBFS, it makes no difference if you configure one rule with multiple ordinals, or multiple rules with one ordinal each. Please note ordinals do not define the order of processing.
- Scope - ACLs generally apply globally. In particular, they are not applied to interfaces. You can however configure an interface as a match criteria.
- Priorities - ACL entry priorities are used to define the processing of multiple matching ACL rules. In RBFS, by default all ACL entries have the same priority, and there is no specific order. For example, if one ACL rule shall permit ICMP traffic from a specific prefix, and another rule shall deny any other ICMP traffic, it will by default result in a conflict as an ICMP packet matches both rules. You can assign a higher priority to the more-specific rule to ensure it will match first.

1.3. Prefix Lists

A prefix list is a named list of prefixes. Instead of listing multiple individual prefixes in a match rule of the ACL itself, you can reference a list that contains the prefixes, and thereby apply a common action to all matching prefixes. This helps to maintain lists and re-use them in multiple ACL rules.

Prefix lists can be used in Access Control List (ACL) for traffic filtering, as well as in Multifield (MF) classifier ACLs. This guide describes how to configure prefix lists, and apply them to user-defined ACLs for traffic filtering. For applying prefix lists to MF classifiers, please refer to the HQoS configuration guide.

When a prefix list is configured and referenced in an ACL, it is internally first added to an intermediate ACL configuration table. For each prefix, one separate rule is added to the final ACL configuration table. This is different from a prefix match in the ACL rule itself that is directly added to the ACL configuration table. A dedicated range of ordinals (200001-4294967295) is reserved to expand ACL rules when using prefix lists. If configured, the priority will be copied from the prefix list ACL configuration to all the expanded ACL rules.

When using prefix lists, the following restrictions apply:

- You cannot configure the same prefix list name to match the source prefix list and destination prefix list.
- You cannot configure both source prefix and source prefix list on the same ACL configuration.
- You cannot configure both destination prefix and destination prefix list on the same ACL configuration.

1.4. Supported Platforms

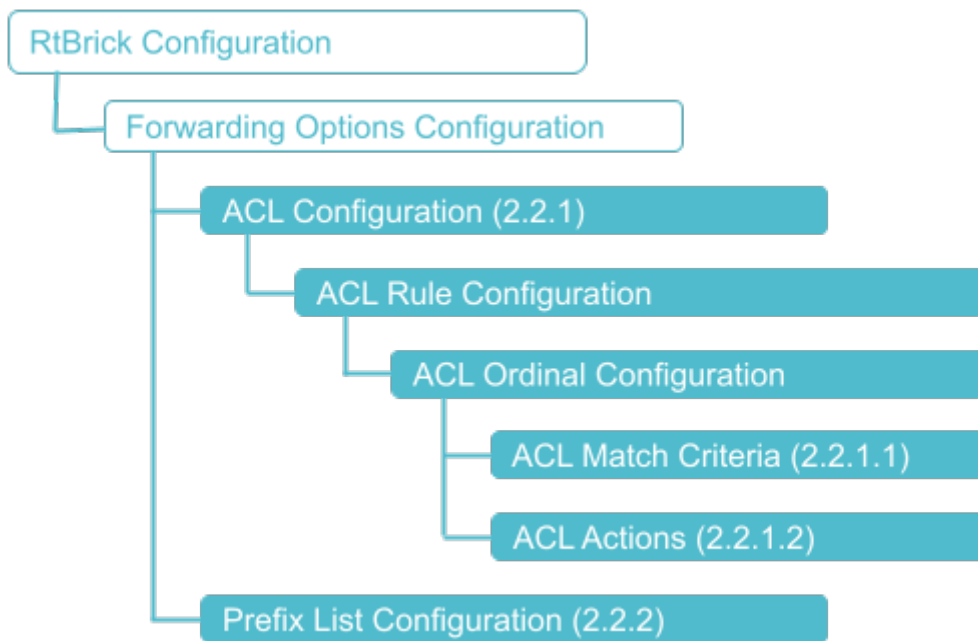
Not all features are necessarily supported on each hardware platform. Refer to the Platform Guide for the features and the sub-features that are or are not supported by each platform.

2. Configuring Access Control Lists

For configuring an access control list, you define a filter criteria (with match conditions) for the packets and an action for the device to take if the packets match the filtering criteria.

2.1. Configuration Hierarchy

The diagram illustrates the ACL configuration hierarchy.



2.2. Configuration Syntax and Commands

The following sections describe the ACL configuration syntax and commands.

2.2.1. Configuring ACLs

Syntax:

```
set forwarding-options acl [I2 | I3v4 | I3v6] rule <name> ordinal <number>
<option> <attribute> <value>
```

| Options | Description |
|-------------|--|
| <name> | Name of the ACL rule. |
| <number> | Specifies the ordinal number. |
| match <...> | Match configuration hierarchy. Please refer to section 2.2.1.1 for the ACL match criteria configuration. |

| Options | Description |
|---------------------|---|
| action <...> | Action configuration hierarchy. Please refer to section 2.2.1.2 for the ACL actions configuration. |
| priority <priority> | Specifies the ACL priority value. The default entry priority for user-defined ACLs changes to 500. The configurable ACL entry priority range becomes 100 - 20000. |

2.2.1.1. Configuring ACL Match Criteria

set forwarding-options acl [l2 | l3v4 | l3v6] rule <rulename> ordinal <ordinal_value> match <attribute> <value>

| Attribute | Description |
|---|--|
| destination-mac <destination-mac> | ACL L2 destination mac match. |
| destination-ipv4-prefix <destination-ipv4-prefix> | ACL L3 IPv4 destination prefix match. |
| destination-ipv4-prefix-list <destination-ipv4-prefix-list> | ACL destination IPv4 prefix list name. You can apply a prefix-list that is previously configured. Refer to section [configure-prefix-list] . |
| destination-l4-port <destination-l4-port> | ACL L4 destination port match. |
| destination-ipv4-local [true false] | Indicates whether match support is enabled for all traffic destined for the routers' IP addresses |
| destination-ipv6-prefix <destination-ipv6-prefix> | ACL L3 IPv6 destination prefix match. |
| destination-ipv6-prefix-list <destination-ipv6-prefix-list> | ACL destination IPv6 prefix list name. You can apply a prefix-list that is previously configured. Refer to section [configure-prefix-list] . |
| destination-ipv6-local [true false] | Indicates whether match support is enabled for all traffic destined for the routers' IP addresses |
| direction ingress | ACL L2/L3 direction match. Currently, only the ingress direction is supported. |
| ethertype <ethertype> | ACL L2 EtherType match. |
| inner-tag-protocol-id <inner-tag-protocol-id> | ACL L2 inner TPID match. |
| inner-vlan <inner-vlan> | ACL L2 inner-VLAN match. |
| inner-vlan-cfi <inner-vlan-cfi> | ACL L2 inner-VLAN CFI match. |

| Attribute | Description |
|---|---|
| inner-vlan-priority <inner-vlan-priority> | ACL L2 inner-VLAN priority match. |
| interface <interface> | Interface match. |
| ip-options true | Match if IPv4 packet has options. Supported value: true. |
| ip-protocol <protocol> | ACL IP protocol value match such as TCP, UDP, ICMP. |
| ipv4-dscp <ipv4-dscp> | IPv4 DSCP value. |
| ipv4-tos <ipv4-tos> | IPv4 ToS value. |
| ipv6-tc <ipv6-tc> | Codepoint class value. |
| logical-interface <logical-interface> | Logical interface match. |
| source-ipv4-prefix <source-ipv4-prefix> | ACL L3 IPv4 source prefix match. |
| source-ipv4-prefix-list <source-ipv4-prefix-list> | ACL source IPv4 prefix list name. You can apply a prefix-list that is previously configured. Refer to section [configure-prefix-list] . |
| source-ipv6-prefix <source-ipv6-prefix> | Configure ACL L3 IPv6 source prefix match. |
| source-ipv6-prefix-list <source-ipv6-prefix-list> | ACL source IPv6 prefix list name. You can apply a prefix-list that is previously configured. Refer to section [configure-prefix-list] . |
| source-l4-port <source-l4-port> | ACL L4 source port match. |
| outer-tag-protocol-id <outer-tag-protocol-id> | ACL L2 outer TPID match. |
| outer-vlan <outer-vlan> | ACL L2 outer-VLAN match. |
| outer-vlan-cfi <outer-vlan-cfi> | ACL L2 outer VLAN CFI match. |
| outer-vlan-priority <outer-vlan-priority> | ACL L2 outer VLAN priority match. |
| source-mac <source-mac> | ACL L2 source MAC match. |
| traffic-class <class> | Forward class value. Supported values: class-0 to class-7, class-all. |
| ttl <ttl> | IPv4 time-to-live value. |

Example 1: Layer 2 Match Configuration

```
{
  "rtbrick-config:acl": {
    "l2": {
      "rule": [
        {
          "rule-name": "a10nsp-drop-lag-2",
          "ordinal": [
            {
              "ordinal-value": 1,
              "match": {
                "direction": "ingress",
                "interface": "lag-2",
                "outer-vlan-priority": 1
              },
              "action": {
                "drop": "true",
                "statistics": "true"
              }
            }
          ],
        }
      ],
    }
  }
}
```

Example 2: Layer 3 IPv4 Match Configuration

```
{
  "rtbrick-config:acl": {
    "l3v4": {
      "rule": [
        {
          "rule-name": "rtb_firewall_two",
          "ordinal": [
            {
              "ordinal-value": 1000,
              "match": {
                "direction": "ingress",
                "source-ipv4-prefix": "40.1.1.0/24",
                "source-l4-port": 8080
              },
              "action": {
                "drop": "true"
              }
            }
          ]
        },
        {
          "rule-name": "rule2",
          "ordinal": [
            {
              "ordinal-value": 5,
              "match": {
                "direction": "ingress",
                "interface": "ifp-0/0/1"
              }
            }
          ]
        }
      ]
    }
  }
}
```

Example 3: Layer 3 IPv6 Match Configuration

```
{
  "rtbrick-config:l3v6": {
    "rule": [
      {
        "rule-name": "rtb_firewall_two",
        "ordinal": [
          {
            "ordinal-value": 1000,
            "match": {
              "direction": "ingress",
              "source-ipv6-prefix": "40::0/64",
              "source-l4-port": 8080
            },
            "action": {
              "permit": "true"
            }
          }
        ]
      }
    ]
  }
}
```

Example 4: Match support for all traffic destined any of the routers IP addresses

```

supervisor@acl>sudo: cfg> show config forwarding-options acl
{
  "rtbrick-config:acl": {
    "l3v4": {
      "rule": [
        {
          "rule-name": "rule4",
          "ordinal": [
            {
              "ordinal-value": 4,
              "match": {
                "direction": "ingress",
                "destination-ipv4-local": "true"
              },
              "action": {
                "drop": "true"
              }
            }
          ]
        }
      ]
    },
    "l3v6": {
      "rule": [
        {
          "rule-name": "rule2",
          "ordinal": [
            {
              "ordinal-value": 2,
              "match": {
                "direction": "ingress",
                "destination-ipv6-local": "true"
              },
              "action": {
                "drop": "true"
              }
            }
          ]
        }
      ]
    }
  }
}

```


2.2.1.2. Configuring ACL Actions

Syntax:

```

set forwarding-options acl [l3v4 | l3v6] rule <rulename> ordinal
<ordinal_value> action <attribute> <value>

```

| Attribute | Description |
|--------------------------------|---|
| drop [true/false] | Configure action, drop packets. True indicates that the specified action is performed. False indicates that the specified action is not performed. |
| permit [true/false] | Configure action, permit packets. True indicates that the specified action is performed. False indicates that the specified action is not performed. |
| action statistics [true/false] | Configure action, enable statistics. <div style="display: flex; align-items: center;">  <p>A limited number of counter resources are available in a common pool of counter resources for user-defined ACLs, protocol ACLs, L3, and L2X logical interfaces.</p> </div> |
| forward-class <class> | Specifies forward class value (class-0 to class-7, class-all) |
| mirror <mirror> | Specifies ACL action mirror name. |
| capture [true/false] | You can enable the capture action when using the RBFS built-in capture feature with an ACL to more granularly specify the traffic to be captured. For more information and an example, refer to the <i>RBFS NOC Troubleshooting Guide</i> . |
| policer-name <policer-name> | Specifies policer profile name. |
| redirect-to-cpu [true/false] | Configure action, redirect packets to CPU. |

Example

```
{
  "rule-name": "rtb_firewall_two",
  "ordinal": [
    {
      "ordinal-value": 1000,
      "match": {
        "direction": "ingress",
        "source-ipv4-prefix": "40.1.1.0/24",
        "source-l4-port": 8080
      },
      "action": {
        "drop": "true"
      }
    }
  ]
}
```

Configuring Prefix Lists

Configuring IPv4/IPv6 Prefix List for ACL and Multifield Classifier

Syntax:

set forwarding-options prefix-list <prefix-list-name> <attribute> <value>

| Attribute | Description |
|---------------------------|--|
| <prefix-list-name> | Name of the prefix list which will be later used to attach with ACL configuration. |
| ipv4-prefix <ipv4_prefix> | Specifies the IPv4 prefix address. |
| ipv6-prefix <ipv6_prefix> | Specifies the IPv6 prefix address. |

Example

```
{
  "rtbrick-config:prefix-list": [
    {
      "prefix-list-name": "ipv4-list",
      "ipv4-prefix": [
        {
          "ipv4-prefix": "40.1.1.0/24"
        },
        {
          "ipv4-prefix": "50.1.1.0/24"
        },
        {
          "ipv4-prefix": "60.1.1.0/24"
        }
      ]
    }
  ]
}
```

3. Operational Commands

3.1. ACL Show and Statistics Commands



ACL statistics are currently not supported for PIM, IGMP, and L2TP protocol traffic.

Syntax:

show acl <option>

| Option | Description |
|-----------------------|--|
| - | Without any option, this command displays brief information about access-control list (ACL). |
| detail | Displays detailed information about access-control list (ACL). |
| <acl-rule-name> | Displays detailed information for a specified ACL rule name. |
| statistics | Displays ACL statistics information. |
| <acl-name> statistics | Displays ACL statistics information for the specified ACL. |

Example 1: Show information about ACLs

```

supervisor@rtbrick>LEAF01: op> show acl
ACL                Ordinal    Type        Attach Point
rule4              4          13v4        -
                  8          13v4        -
lldp.ifp-0/0/0.trap.rule  -          12          ifp-0/0/0
lldp.ifp-0/1/0.trap.rule  -          12          ifp-0/1/0
lldp.ifp-0/1/1.trap.rule  -          12          ifp-0/1/1
lldp.ifp-0/1/4.trap.rule  -          12          ifp-0/1/4
lldp.ifp-0/1/5.trap.rule  -          12          ifp-0/1/5
lldp.ifp-0/1/6.trap.rule  -          12          ifp-0/1/6
lldp.ifp-0/1/12.trap.rule -          12          ifp-0/1/12
lldp.ifp-0/1/13.trap.rule -          12          ifp-0/1/13
lldp.ifp-0/1/22.trap.rule -          12          ifp-0/1/22
lldp.ifp-0/1/23.trap.rule -          12          ifp-0/1/23

```

Example 2: Show detailed information about ACLs

```

supervisor@rtbrick>LEAF01: op> show acl detail
Rule: rule4
  ACL type: 13v4
  Ordinal: 4

```

```

Match:
  Direction: ingress
  Source IPv4 prefix: 4.4.4.4/32
Action:
  Drop: True
Result:
  Trap ID: User Defined
Statistics:
  Units      Total      Accepted   Dropped
  Packets    4          0          4
  Bytes     424        0          424
Ordinal: 8
Match:
  Direction: ingress
  Source IPv4 prefix: 8.8.8.8/32
Action:
  Drop: True
Result:
  Trap ID: User Defined
Statistics:
  Units      Total      Accepted   Dropped
  Packets    9          0          9
  Bytes     990        0          990
Rule: lldp.ifp-0/0/0.trap.rule
ACL type: 12
Ordinal: -
Match:
  Attachment point: ifp-0/0/0
  Direction: ingress
  Destination MAC: 01:80:c2:00:00:0e
Action:
  Redirect to CPU: True
Result:
  Trap ID: LLDP
Statistics:
  Units      Total      Accepted   Dropped
  Packets    105        105        0
  Bytes     12915      12915      0
Rule: lldp.ifp-0/1/0.trap.rule
ACL type: 12
Ordinal: -
Match:
  Attachment point: ifp-0/1/0
  Direction: ingress
  Destination MAC: 01:80:c2:00:00:0e
Action:
  Redirect to CPU: True
Result:
  Trap ID: LLDP
Statistics:
  Units      Total      Accepted   Dropped
  Packets    220        220        0
  Bytes     19140      19140      0

```

Example 3: Show detailed information for a specified ACL Rule


```
supervisor@rtbrick>LEAF01: op> show acl rule4
Rule: rule4
  ACL type: 13v4
  Ordinal: 4
  Match:
    Direction: ingress
    Source IPv4 prefix: 4.4.4.4/32
  Action:
    Drop: True
  Result:
    Trap ID: User Defined
  Statistics:
    Units      Total      Accepted   Dropped
    Packets    4         0         4
    Bytes      424       0         424
Ordinal: 8
  Match:
    Direction: ingress
    Source IPv4 prefix: 8.8.8.8/32
  Action:
    Drop: True
  Result:
    Trap ID: User Defined
  Statistics:
    Units      Total      Accepted   Dropped
    Packets    9         0         9
    Bytes      990       0         990
```

Example 4: Display ACL statistics information

```

supervisor@rtbrick>LEAF01: op> show acl statistics
ACL                Units      Total      Accepted   Dropped
rule4              Packets    4          0          4
                  Bytes     424        0          424
rule4              Packets    9          0          9
                  Bytes     990        0          990
lldp.ifp-0/0/0.trap.rule Packets    107        107        0
                  Bytes    13161     13161     0
lldp.ifp-0/1/0.trap.rule Packets    221        221        0
                  Bytes    19227     19227     0
lldp.ifp-0/1/1.trap.rule Packets    221        221        0
                  Bytes    19227     19227     0
lldp.ifp-0/1/4.trap.rule Packets    214        214        0
                  Bytes    31672     31672     0
lldp.ifp-0/1/5.trap.rule Packets    214        214        0
                  Bytes    31672     31672     0
lldp.ifp-0/1/6.trap.rule Packets    214        214        0
                  Bytes    31672     31672     0
lldp.ifp-0/1/12.trap.rule Packets    107        107        0
                  Bytes    13375     13375     0
lldp.ifp-0/1/13.trap.rule Packets    107        107        0
                  Bytes    13375     13375     0
lldp.ifp-0/1/22.trap.rule Packets    107        107        0
                  Bytes    13375     13375     0
lldp.ifp-0/1/23.trap.rule Packets    107        107        0
                  Bytes    13375     13375     0

```

Example 5: Display ACL statistics information for the specified ACL

```

supervisor@rtbrick>LEAF01: op> show acl rule4 statistics
ACL      Units      Total      Accepted   Dropped
rule4    Packets    4          0          4
         Bytes     424        0          424
rule4    Packets    9          0          9
         Bytes     990        0          990

```