ACL (Access Control List)

An access control list (ACL) is an access control list based on an access control matrix. Access control sequences consist of access control entries (ACEs).

Restriction:
[202111.0] Known issue:
[SONIC-4734] the command of the ACL table for Control Plane CANNOT be applied.
[SONIC-4684] [Intel TF/TF2] Fix the problem that ACL with priority 1 will be matched as the highest rule. (This issue is fixed on 202111.1)
[SONIC-5519] Fix the problem that MCLAG session cannot be established after rebooting with control plane ACL. (This issue is fixed on 202111.3)
[SONIC-7922] Fix the issue of DHCP Broadcast/Unicast packets being incorrectly forwarded to the peer leaf switch when CACL is applied. (This issue is fixed on 202111.8)
There is no SONiC command to add ACL rules. (After 202111.5, it is supported to use command to add ACL, but unsupported for Control Plane ACL)
EC SONiC default configuration is "permit all".
LAG's member port shall not be added to the ACL Tables or will be considered as invalid configuration and return fail.
LAG ACL configurations will be automatically applied to all the LAG members.
Control Plane ACL:
Support services for SSH/SNMP.
When the Control Plane ACL is running, the un-list service will be denied. i.e If the ACL table bind with SSH, SNMP will be denied.
There is **in the last rules automatically.**
Matching criteria("V" is valid matching criteria, "X" is invalid matching criteria)
The VLAN egress ACL can not be used on an egress port with a VLAN untagged member. It only supports the tagged member port.

	CTRLPLANE
protocol	X
source-ip-address	V
destination-ip-address	X
tcp_flags	V
source-port	X
destination-port	X
dscp	X

(ICMP) type   X
(ICMP) code   X
The ACL support table is shown below:

ACL
Procedure:
Step 1. Create an ACL table by CLI

```
admin@sonic:~$ sudo config acl add table --help
Usage: config acl add table [OPTIONS] <table_name> <table_type>

 Add ACL table.

 Table type. Available types are L3, L3V6, MIRROR, MIRRORV6,
MIRROR_DSCP,
 CTRLPLANE, and custom defined types.

Options:
 -d, --description TEXT
 -p, --ports TEXT
 -s, --stage [ingress|egress]
 -S, --services TEXT
 --set-policer
 -?, -h, --help                  Show this message and exit.

admin@sonic:~$ sudo config acl add table ACL_ETH0 L3 --
description 'drop_1.0' --stage 'ingress' --ports 'Ethernet0'
```

Note:

The "policy_desc" is a string about the description of ACL table.
The "stage" is about the ACL direction.
Ingress
egress
Support :
L3
L3V6
MIRROR(About the MIRROR, please refer to this article.)
CTRLPLANE(refer to Service ACL)
Step 2. Check ACL table by SONiC command.

```
admin@sonic:~$ show acl table
Name       Type    Binding    Description    Stage    Policer
--------  ------  ---------  -------------  -------  ---------
```

```
ACL_ETH0  L3      Ethernet0  drop_1.0       ingress
```

Step 3. Create the JSON file(ACE.json) for ACL rules and apply with command

```
admin@sonic:~$ sudo vi ACE.json
{
   "ACL_RULE": {
       "ACL_ETH0|ACE_DROP2": {
           "PACKET_ACTION": "DROP",
           "PRIORITY": "1",
           "DST_IP": "192.168.1.11/32",
           "IP_TYPE": "IP"
    },
       "ACL_ETH0|ACE_DROP1": {
           "PACKET_ACTION": "DROP",
           "PRIORITY": "2",
           "SRC_IP": "192.168.1.10/32",
           "IP_TYPE": "IP",
           "L4_SRC_PORT": "53"
       }
   }
}
admin@sonic:~$ sudo config load ACE.json -y
```

After version 202111.5, the ACL rule can be added by sonic command, based on the ACE.json above, the corresponding command is below.

```
admin@sonic:~$ sudo config acl add rule --priority 1 --dst-ip4
192.168.1.11/32 ACL_ETH0 deny
admin@sonic:~$ sudo config acl add rule --priority 2 --src-l4-
port 53 --src-ip4 192.168.1.10/32 ACL_ETH0 deny
Caution: Not support IP_TYPE : IP by Sonic command
admin@sonic:~$ sudo config acl add rule --dst-ip
Usage: config acl add rule [OPTIONS] <table_name> [permit|deny]
Try "config acl add rule -h" for help.

Error: no such option: --dst-ip (Possible options: --dst-ip4, --
dst-ip6)
```

Note:

Key "ACL_ETH0|ACE_DROP2" and "ACL_ETH0|ACE_DROP1" are the names of rules of ACL ACL_ETH0.
If key "types" of ACL TABLE is L3 or L3V6,
Key in ACL rule is "PACKET_ACTION"
The value of "PACKET_ACTION" is FORWARD or DROP.

If key "types" of ACL table is MIRROR,
Key in ACL rule is "MIRROR_ACTION"
The value of "MIRROR_ACTION" is the name of mirror session
The number of priority is bigger which means priority is high.
Take the above example, the priority 2 will match first.
Caution: There's a known issue on version 202111.0, the priority of the Tofino platform(Wedge100bf series, 9516-32D), The number of priority is smaller which means priority is high. (This issue is fixed on 202111.1)
Here are the values for "IP_TYPE":
ANY Filter IPv4, IPv6, Ether type
IP   Filter IPv4, IPv6
NON_IP   Filter Ether type only
IPV4ANY   Filter IPv4 only
NON_IPv4 Filter IPv6, Ether type
IPV6ANY   Filter IPv6 only
NON_IPv6 Filter IPv4, Ether type
ARP Filter ARP request, reply
ARP_REQUEST   Filter ARP request only
ARP_REPLY Filter ARP reply only
Caution: NON_IP, NON_IPv4, NON_IPv6, ARP_REQUEST, ARP_REPLY could not work now.
Other keys(parameters):
DST_IP example: "DST_IP": "192.168.1.10/32"
SRC_IPV6 example: "SRC_IPV6": "2001::db:1"
Caution: The type of the ACL table should be modified to "L3V6"
DST_IPV6 example: "DST_IPV6": "2001::db:2"
Caution: The type of the ACL table should be modified to "L3V6"
ETHER_TYPE example: "ETHER_TYPE": "0x842" or "ETHER_TYPE": "2114"
L4_SRC_PORT example: "L4_SRC_PORT": "53"
L4_DST_PORT example: "L4_DST_PORT": "53"
IP_PROTOCOL example: "IP_PROTOCOL": "1"
L4_SRC_PORT_RANGE example: "L4_SRC_PORT_RANGE": "1028-4096"
Caution: Egress doesn't support it.
L4_DST_PORT_RANGE example: "L4_DST_PORT_RANGE": "1028-4096"
Caution: Egress doesn't support it.
ICMP_TYPE example: "ICMP_TYPE": "0"
ICMPV6_TYPE example: "ICMPV6_TYPE": "128"
Caution: The type of the ACL table should be modified to "L3V6"
TCP_FLAGS example: "TCP_FLAGS": "16/255"
Note:
FIN =   0x01   "TCP_FLAGS": "0x01/63"
SYN = 0x02   "TCP_FLAGS": "0x02/63"
RST = 0x04   "TCP_FLAGS": "0x04/63"

```
PSH = 0x08      "TCP_FLAGS": "0x08/63"
ACK = 0x10      "TCP_FLAGS": "0x10/63"
URG = 0x20     "TCP_FLAGS": "0x20/63"
Caution: Not support for filtering Congestion Window Reduced
(CWR) and ECN-Echo (ECE)
VLAN_ID, example: "VLAN_ID": "10"
Step 4. Check ACL rules by SONiC command

admin@sonic:~$ show acl rule
Table     Rule        Priority    Action    Match
Status
--------  ---------  ----------  --------
----------------------  --------
ACL_ETH0  ACE_DROP1  2           DROP      IP_TYPE: IP
Active
                                          L4_SRC_PORT: 53
                                          SRC_IP: 192.168.1.10/32
ACL_ETH0  ACE_DROP2  1           DROP      DST_IP:
192.168.1.11/32  Active
                                          IP_TYPE: IP
Control Plane ACL
Procedure:
Step 1. Create an Service ACL table by CLI

admin@sonic:~$ sudo config acl add table CTRL CTRLPLANE --help
Usage: config acl add table [OPTIONS] <table_name> <table_type>

 Add ACL table.

 Table type. Available types are L3, L3V6, MIRROR, MIRRORV6,
MIRROR_DSCP,
 CTRLPLANE, and custom defined types.

Options:
 -d, --description TEXT
 -p, --ports TEXT
 -s, --stage [ingress|egress]
 -S, --services TEXT
 --set-policer
 -h, -?, --help                Show this message and exit.

admin@sonic:~$ sudo config acl add table CTRL CTRLPLANE --
description --services
Note. In 202006 branch, the service ACL table do not have CLI.
Please create a JSON file and apply by
```

```
admin@sonic:~$sudo vi service_table.json
{
: {
        : {
            : ,
            : [
                    ,

            ],
            :
        }
   }
}
admin@sonic:~$ sudo config load service_table.json -y
```

Step 2. Check ACL table by SONiC command.

```
admin@sonic:~$ show acl table
Name    Type        Binding    Description    Stage    Policer
------  ---------  ---------  -------------  -------  ---------
CTRL    CTRLPLANE  SNMP       CTRLPANE ACL   ingress
                   SSH
```

Step 3. Create the JSON file(CTRL_ACE.json) for ACL rules and apply with command

```
admin@sonic:~$ sudo vi CTRL_ACE.json
{
   "ACL_RULE": {
       "CTRL|ACE_ACCEPT": {
           "PACKET_ACTION": "ACCEPT",
           "PRIORITY": "2",
           "SRC_IP": "192.168.1.10/32"
       }
   }
}
admin@sonic:~$ sudo config load CTRL_ACE.json -y
```

Step 4. Check ACL rules by SONiC command

```
admin@sonic:~$ show acl rule
Table    Rule          Priority  Action    Match
Status
-------  ----------  ----------  --------
----------------------  --------
CTRL     ACE_ACCEPT           2  ACCEPT    SRC_IP:
192.168.1.10/32  Active
```