WHITE PAPER

Tech Talk | Access Control List

Prevent attacks from TRUSTED users and devices.

MOXA®

Reliable Networks ▲ Sincere Service

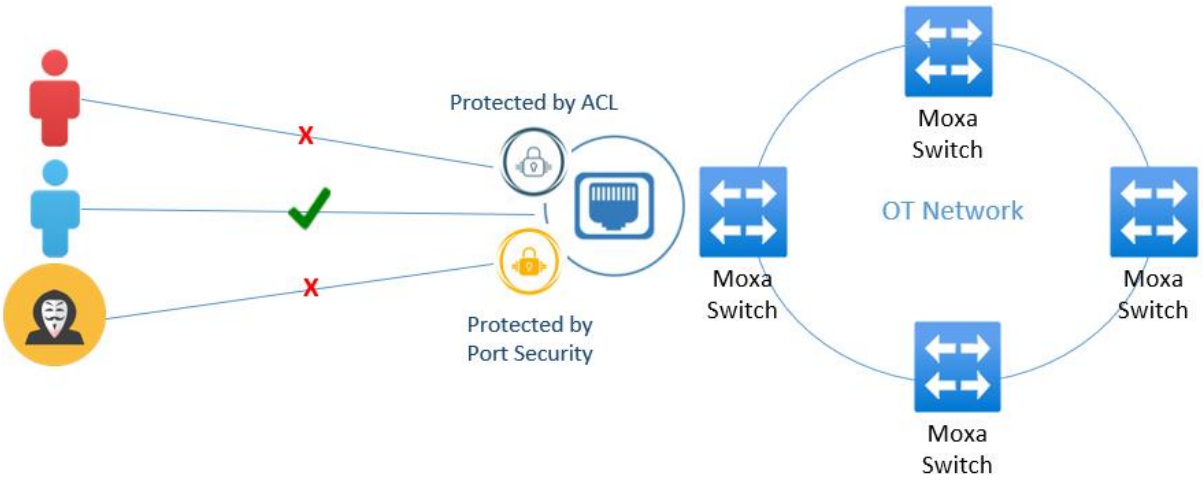
ecs

Tech Talk | Access Control List (ACL)

Why we need ACLs?

If Port Security is good enough to protect infrastructure like managed switches, why do we still need more? Here's why ACLs are essential:

- **Port Security** prevents attacks from **UNTRUSTED** users or devices.
- **Access Control Lists (ACLs)** protect against attacks from **TRUSTED** users or devices that may be compromised.



What action can ACLs perform?

Access Control Lists (ACLs) function like a security guard at the entrance or exit of an Ethernet port, constantly monitoring traffic. Any unauthorized traffic is blocked, preventing it from reaching the other ethernet port, other networks or the management portal. It can permit or deny traffic based on predefined criteria and are applied to ingress ports, egress ports, or VLANs. Acting as hardware-based filters, ACLs ensure efficient traffic control at the hardware level."

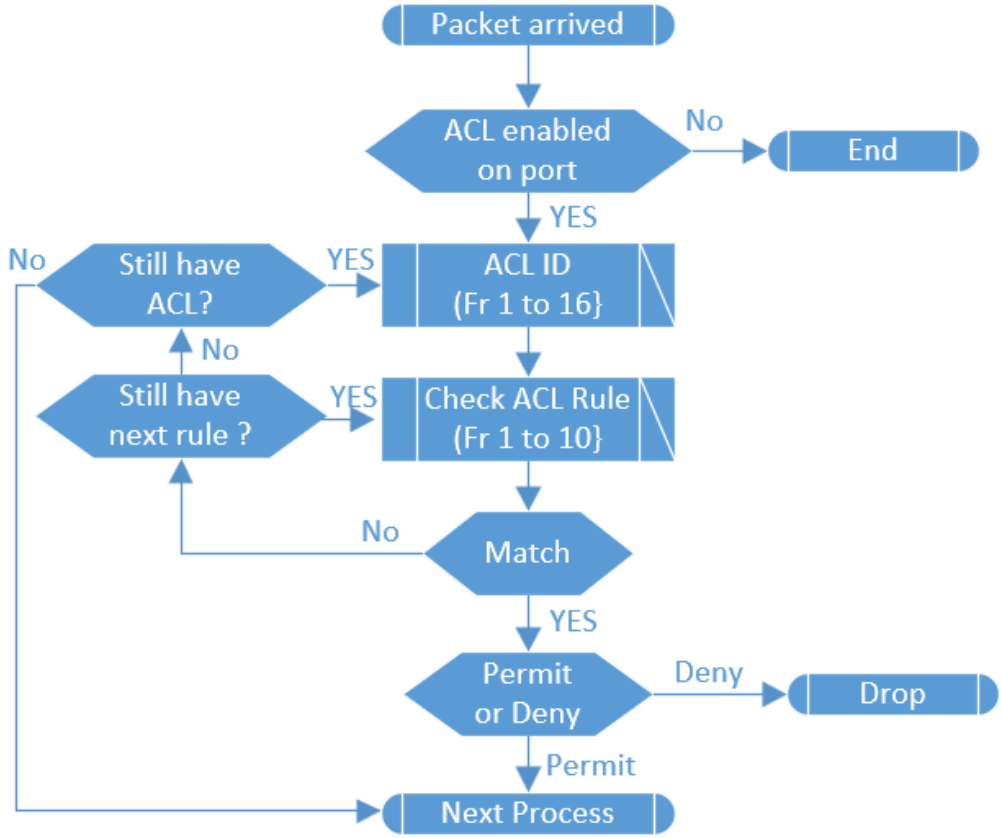
In Ethernet devices like Moxa, ACLs are processed by TCAM (Ternary Content Addressable Memory), a specialized, high-speed memory designed for rapid lookups. TCAM is critical for tasks that require quick decisions based on numerous rules, such as routing, switching, and security filtering.

How TCAM Works:

- Unlike regular memory, which only retrieves data on exact matches, TCAM can match three states: 0, 1, and "don't care" (ternary).

- This ternary capability allows TCAM to efficiently handle exact and wildcard matches, making it ideal for processing rules and policies that require different levels of specificity.

A Moxa switch can support up to 16 ACL IDs, with each ID allowing up to 10 rules. When a packet matches a rule, it will either be dropped or forwarded accordingly. By default, the ACL rule permits traffic from any source to any destination.



Two types of ACLs (IP-based ACL & MAC-based ACL)

IP-based ACL and **MAC-based ACL** are both used to control access to network resources, but they differ in their focus and operational layers within the OSI model.

Comparison:

Feature	IP-based ACL	MAC-based ACL
Layer	Layer 3 (Network) / Layer 4 (Transport)	Layer 2 (Data Link)
Control	IP Protocols: ARP, ICMP, IGMP, TCP, UDP, Source IP & Mask Destination IP & Mask TCP/UDP: Source Port TCP/UDP: Destination Port DSCP	Source MAC addresses & Mask Destination MAC addresses & Mask Ethernet Type (protocol): 0x0000 ~ 0xFFFF VLAN ID: 1 ~ 4094 CoS: 0 ~ 7
Use Case	Network/subnet-level access control	Device-level access control in local networks
Flexibility	Can define rules for specific services	Device-specific, but not protocol-specific

Feature	IP-based ACL	MAC-based ACL
Security	Better for broader network security	Can be bypassed via MAC address spoofing
Scalability	More scalable for large networks	Limited scalability in larger networks
Pros	**Granular Control**: You can filter traffic based on IP addresses, protocols (TCP, UDP, ICMP), and even port numbers. **Cross-Network**: Can control traffic between different networks, such as local area networks (LANs) and wide area networks (WANs). **Common in Firewalls**: Frequently used to enforce network security policies, control traffic to/from specific IP ranges, and limit access to specific services (e.g., block HTTP traffic on port 80). **Dynamic Addressing**: Works well in environments with dynamic IP allocation (DHCP).	**Device-Specific Control**: Controls access at the device level, regardless of the IP address. Useful for ensuring only certain devices can connect to the network. **Works in DHCP Environments**: Since MAC addresses do not change (unlike IP addresses), they remain constant even when IP addresses are dynamically assigned. **Simpler in Local Networks**: It's effective in smaller or local networks where you want to enforce device-specific access controls.
Cons	**IP Address Changes**: If devices change IP addresses frequently (dynamic IP addressing), ACLs need updating or could allow/deny unintended traffic. **Scalability Issues**: Managing large sets of IP addresses can become complex in larger networks.	**Limited to Local Networks**: MAC-based ACLs only work in local area networks (LANs) since MAC addresses are not transmitted across network boundaries (Layer 2 only). **MAC Spoofing**: MAC addresses can be easily spoofed, so this is not a highly secure method for controlling access. **Scalability**: Managing MAC address lists can be cumbersome in large networks, especially when adding or removing devices frequently.

Use Cases:

- **IP-based ACL**:
  - Controlling access between different subnets, VLANs, or networks.
  - Filtering traffic between internal and external networks (e.g., internet access control).
  - Allowing or blocking specific services (e.g., web, FTP, etc.) based on port numbers or protocols.
- **MAC-based ACL**:
  - Controlling access to the network based on device-specific hardware addresses.
  - Used in switches, wireless access points, or routers to ensure only known devices can connect to the network.
  - Common in smaller, more controlled environments like offices, small businesses, or homes where devices can be manually added to the ACL.

In many scenarios, both types of ACLs can be combined for enhanced security.

QoS ACL

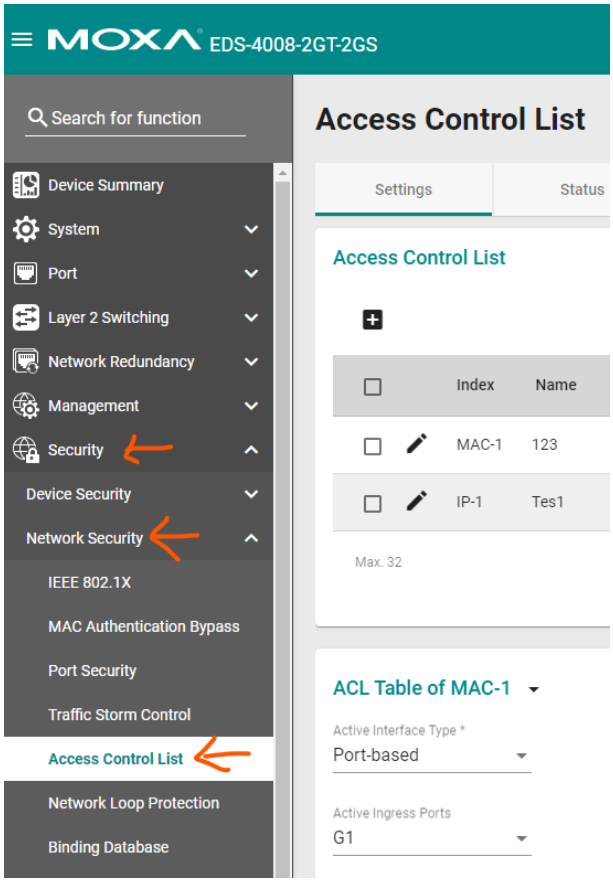
If using IP based, it can remark outgoing DSCP value to permit the packet remark DSCP in the action.

This feature is supported on the following models: -

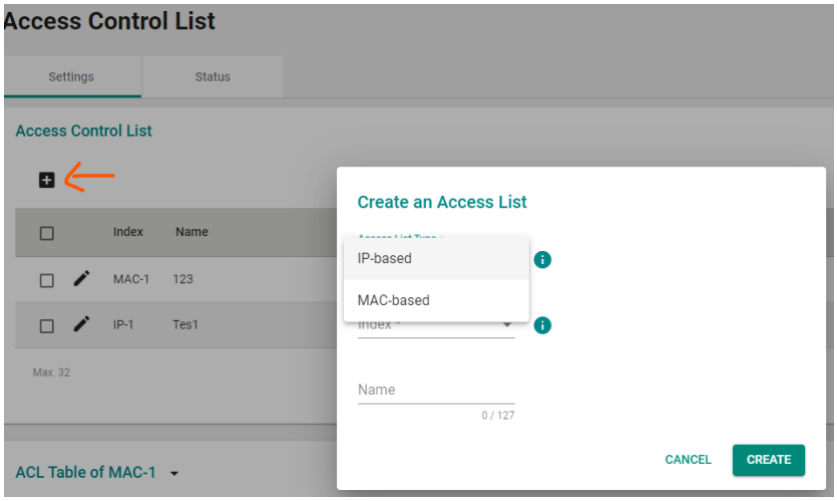
- ICS-G78xx series: https://express.ecsnz.com/en/ics-g78xx-layer-3
- IKS-G6824A series: https://express.ecsnz.com/en/iks-g6524-series
- EDS-G500E series: https://express.ecsnz.com/en/gigabit-managed
- EDS-G4000 series: https://express.ecsnz.com/en/eds-g4000
- MDS-G4000 series: https://express.ecsnz.com/en/mds-g4000

How to Configure this feature in EDS-4008-2GT-2GS

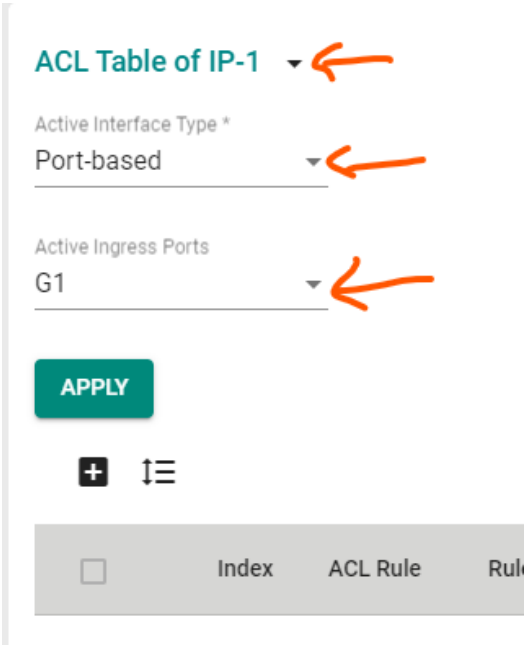
1. Navigate the menu under **Security** > **Network Security** > **Access Control List**



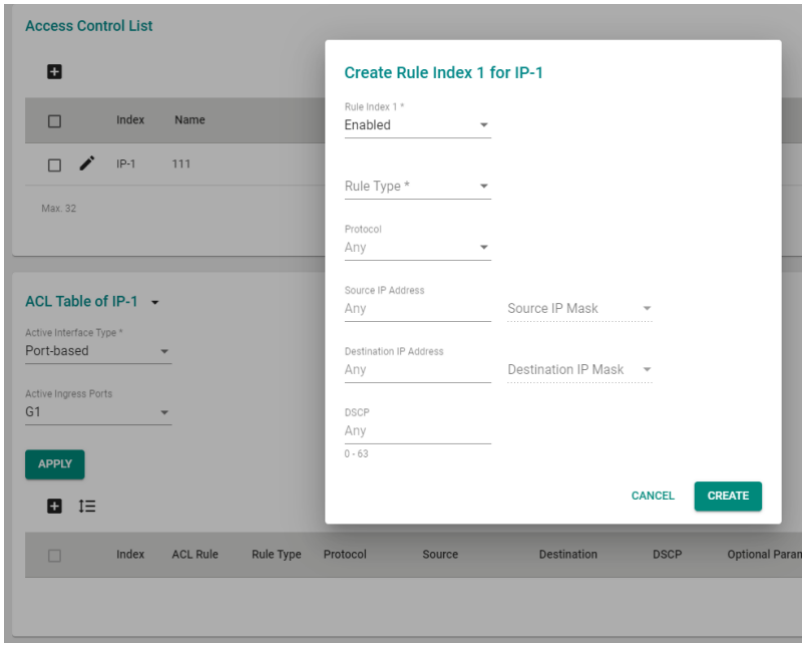
2. To select the IP-based
    a. Select the Settings tab and click the “+” icon to select IP-based or MAC-based and select the index no and insert the Name. Then press “Create”.



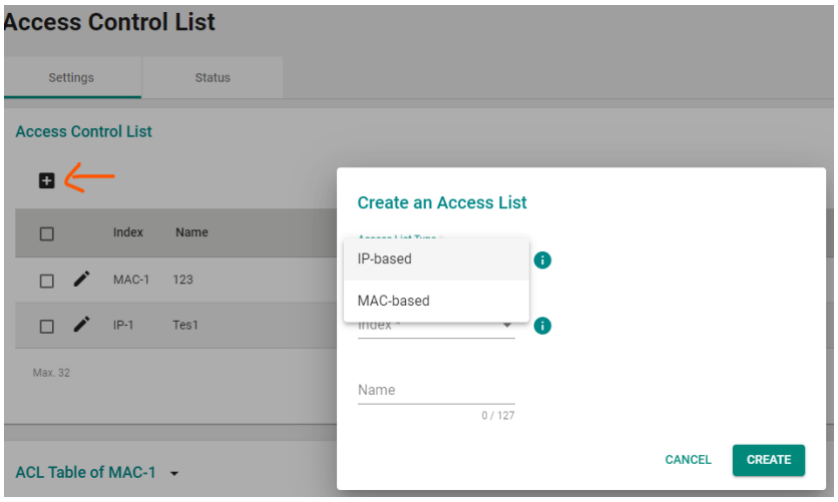
b. Select the ACL Table no, port based + the Active Ingress Ports on VLAN or Vlan based + Active ingress VLAN and click “Apply”



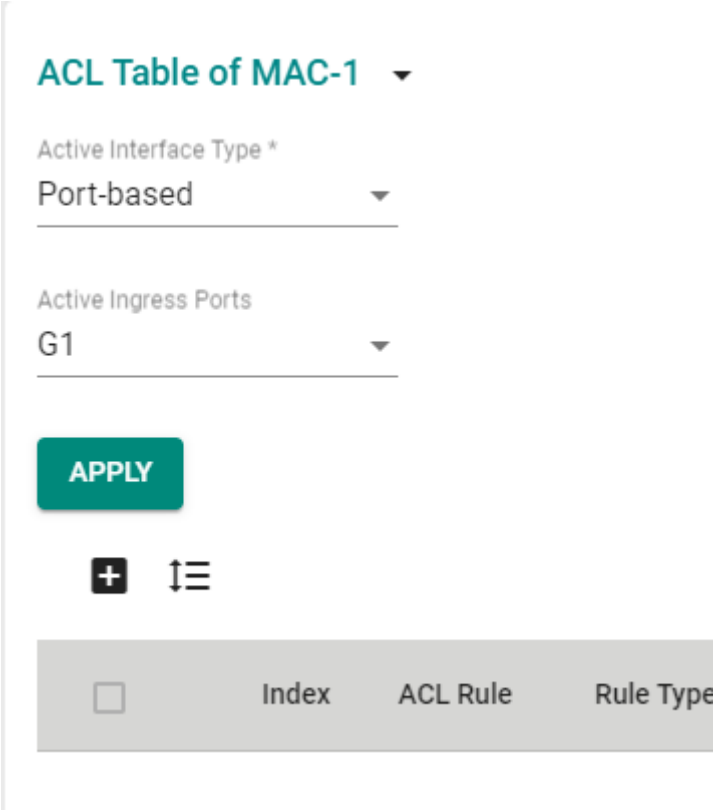
c. Click the “+” icon to create Rule index and fill in the details



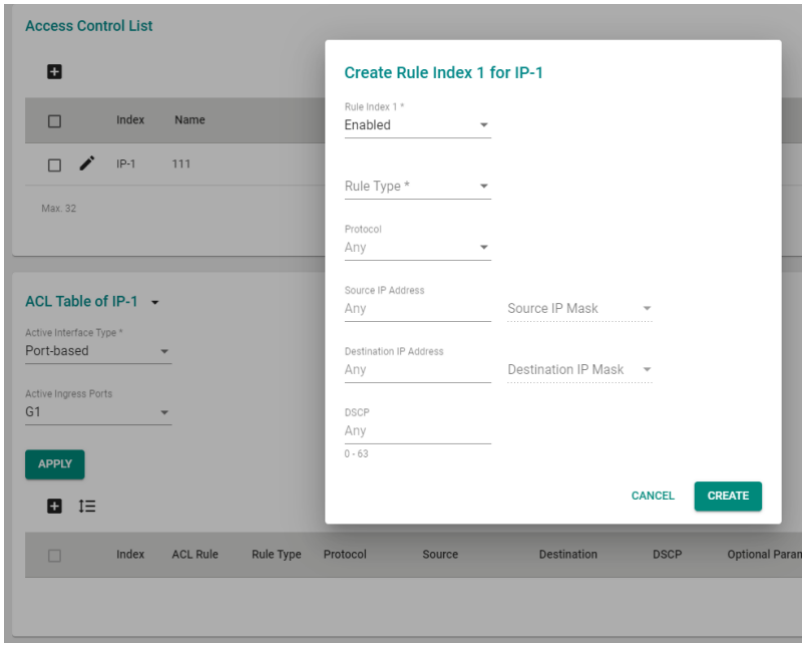
3. To select the MAC-based
    a. Select the Settings tab and click the "+" icon to select IP-based or MAC-based and select the index no and insert the Name. Then press "Create".



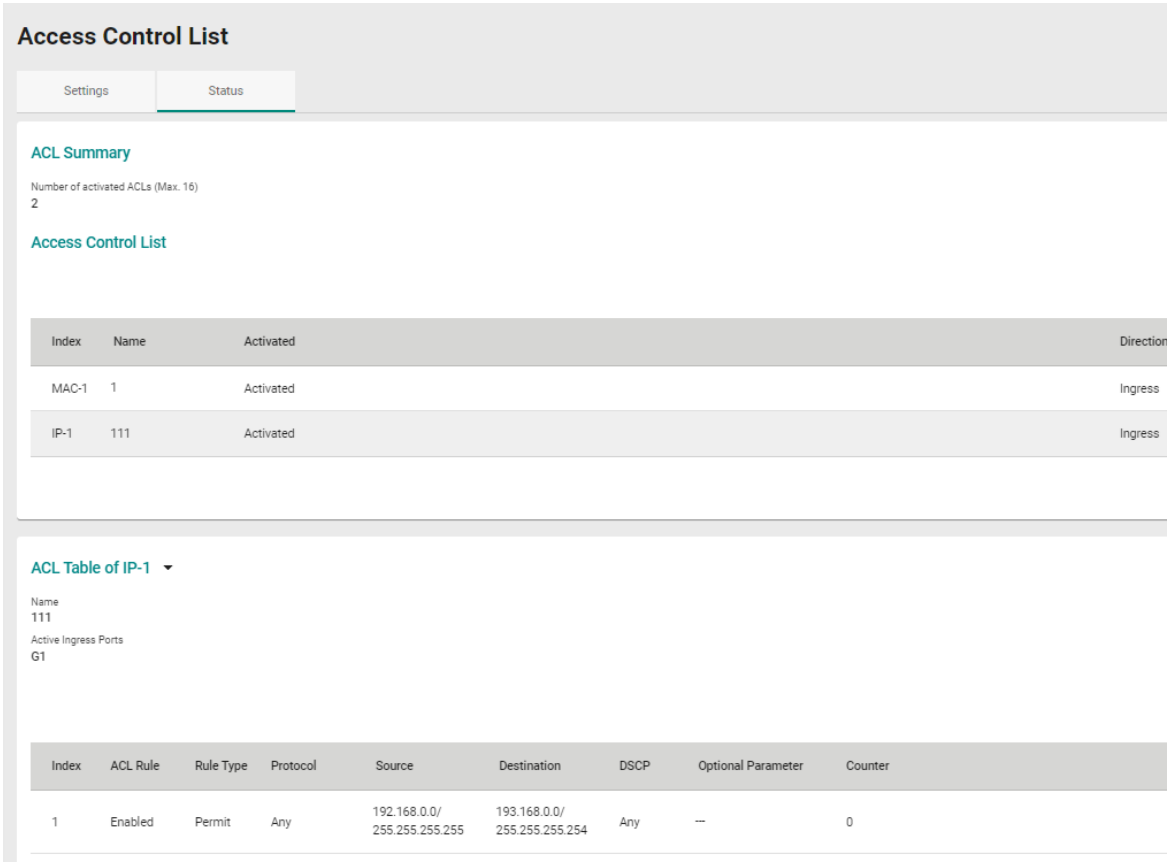
    b. Select the ACL Table no, port based + the Active Ingress Ports on VLAN or Vlan based + Active ingress VLAN and click "Apply"



    c. Click the "+" icon to create Rule index and fill in the details



4. After you configure the ACL, you can go to Status to check what you configured earlier.



Most Moxa managed switches support Access Control List. Additionally, the GUI may vary between different switch models. For more detailed information, please refer to the specific manual for each switch.

Please contact automation@ecsnz.com if you have any questions.

--- END ---