

ACL restrictions on IP addresses accessing the switch



Overview

3) ACL can filter either L2 or L3 fields, (L2/L3 source and destination addresses, protocol, VLAN ID and priority or TCP port).

Key Takeaways

A VACL filters traffic entering the switch on the VLANs to which it is assigned. At a minimum an ACL must have one, explicit "permit" or "deny" Access Control Entry. This document describes various types of IP Access Control Lists (ACLs) and how they can filter network traffic. There are no specific prerequisites for this document. Some of these are present since Cisco IOS ® Software Releases 8. After you specify an access control list, the Autonomous AI Database only accepts connections from addresses on the access control list and the database rejects all other client. An Access Control List (ACL) consists of one rule or a set of rules that describe the packet matching conditions. These conditions include source addresses, destination addresses, and port numbers of packets. This happens by either allowing packets or blocking packets from an interface on a router, switch, firewall etc.



Article Content

How to create Ethernet switch ACL to filter IP addresses

3) ACL can filter either L2 or L3 fields, (L2/L3 source and destination addresses, protocol, VLAN ID and priority or TCP port). The switch does not need to have IP/L3 enabled in order to filter

Related Video Reference

This video was associated with the source search result. Verify technical details against current product documentation and project requirements.

Contact Us

Continue your research online:

Website: <https://thegalleryselfcatering.co.za>

Technical inquiry: <https://thegalleryselfcatering.co.za/contact.html>

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

