Switch blocks MAC access

Article Overview

Switches can block access for specific devices using MAC Lockout, MAC ACLs, or allow/deny lists, with each method offering different levels of control and scalability.

MAC Lockout

MAC Lockout is a feature that allows a switch to deny access to specific MAC addresses across one or multiple ports. It can override port security settings, meaning that even if a MAC address is authorized in port security, it will still be blocked while locked out. MAC Lockout can be applied to a single device or multiple ports simultaneously, providing a flexible way to prevent known devices from connecting to the network. Once a MAC Lockout entry is removed, the switch can re-learn the address according to port security rules .

MAC Access Control Lists (MAC ACLs)

MAC ACLs allow administrators to filter traffic based on MAC addresses at the switch port level. You can configure rules to either allow only specific MAC addresses (allow list) or block certain MAC addresses (deny list). MAC ACLs are useful for controlling access on a per-VLAN or per-port basis and can be applied to multiple devices, but they require careful management to scale across multiple switches .

Allow/Deny Lists

Article Content

Block ARP Packets with Use of MAC Access Lists and VLAN Access

Introduction This document discusses the configuration for a Cisco Catalyst 3550 Series Switch. You can use any Catalyst 2970,

How to Configure MAC ACL: Restrict Access and Filter Traffic on

Get a step-by-step guide on how to configure access restriction and traffic filtering on switch ports using MAC ACL (MAC Access

Configure MAC-Based Access Control List (ACL) and Access Control

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks or allows

Configure MAC-Based Access Control List (ACL) and Access Control

It blocks or allows users to access specific resources. An ACL contains the hosts that are permitted or denied access to the network

How MAC Lockout works

How MAC Lockout works Let us say a customer knows there are unauthorized wireless clients who must not have access to the

Only Allow Specific Clients/Mac addresses | Everything Instant On

The access point can be configured to only allow clients to talk to the default The router allows to configure a list of

Block connections to your Mac with a firewall

Block connections to your Mac with a firewall A firewall can protect your Mac from unwanted contact initiated by other computers

Blocking MAC addresses on switch

Use port-security with protect mode to allow only first learned mac addresses until maximum allowed number is reached and then

How MAC Lockout works

When the wireless clients then attempt to use the network, the switch recognizes the intruding MAC addresses and prevents them

Port security and MAC Lockout

It is possible to use MAC Lockout in conjunction with port-security. You can use MAC Lockout to lock out a single address—deny

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: https://yachtchartercapetown.co.za
Email: info@yachtchartercapetown.co.za
Phone: +27 21 863 4927
Address: 1st Floor, The Towers, 1 St George's Mall, Cape Town, 8001, South Africa

This document is for informational purposes only. Specifications subject to change without notice.