Core switch blocks MAC addresses and blocks traffic



Overview

Port security monitors and blocks Layer 2 traffic on a switch on an individual port basis. Enabling this feature keeps track of permitted source MAC addresses and restricts the number of MACs that can use a specific port. XXXX vlan X drop" My intention was to prevent a single PC from accessing the network. However. I have about ten Cisco switches in my company. I'd like a way to easily apply and centrally manage rules to only allow specific MAC addresses to access any of the ports for any of the VLANs on any of my Cisco switches. This can be a security risk when users connect. MAC filtering is a network access control method where a router or switch allows or blocks devices based on their MAC (Media Access Control) address.

Article Content

How to Block or Allow Several MAC Addresses on All My Cisco Switches

I''d like a way to easily apply and centrally manage rules to only allow specific MAC addresses to access any of the ports for any of the VLANs on any of my Cisco switches. I have the

Introduction to Switch Port Security

Port security monitors and blocks Layer 2 traffic on a switch on an individual port basis. Enabling this feature keeps track of permitted source MAC addresses and restricts the number of

© 2026 EXF OPTICAL NETWORKS - All rights reserved

How to configure port-security on Cisco Switch

In this lesson, you will learn how to configure port security to restrict the number of MAC addresses per port, specify which MAC addresses are allowed, and control what happens when violations occur.

MAC Filtering in Computer Network

MAC filtering is a network access control method where a router or switch allows or blocks devices based on their MAC (Media Access Control) address. When a device tries to join a

cisco Ccnp Switch

The primary function of a Core Layer is to switch traffic as fast as possible and providing connectivity between switch blocks, WAN blocks and/ or any other blocks that may be present.

Native AC Solution: Core Switches Function as the Gateway for Wired

In addition, core switches are configured with the native AC function to manage APs and transmit wireless service traffic on the entire network, implementing wired and wireless convergence.

Port Security

This article describes how to configure port security on Cisco devices to associate specific MAC addresses with the interface.

Switchport Port-Security | NetworkAcademy.IO

Secure your campus LAN access layer with Cisco port security. Learn how to limit MACs, block rogue devices, and recover err-disabled switchports.

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 device. Media Access Control (MAC)-based Access

Blocking MAC address on a Switch

Hello, I have a troublesome computer that someone brings in every night and surfs the Internet, when they should not be. I would like to block their mac address not on just the port,

Configuring Port Blocking

© 2026 EXF OPTICAL NETWORKS - All rights reserved

Port Blocking By default, the switch floods packets with unknown destination MAC addresses out of all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be security

Layer 2 Security Features on Cisco Catalyst Layer 3 Fixed

This document provides a sample configuration for some of the Layer 2 security features, such as port security, DHCP snooping, dynamic Address Resolution Protocol (ARP) inspection and

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

You can filter on this protocol type as interesting traffic for the access list. In global configuration mode, create a named MAC extended access list with the name ARP_Packet. Enter

MAC Address-Based Traffic Blocking

Hi, Since MAC Address-Based Traffic Blocking does not work with Multicast address(ipv6mcast), is there a way to achieve the same in another way. If it ''s not possible i can do

Block internet access based on MAC address

Block internet access based on MAC address Mar 5, 2024 MAC address filtering is more secure than IP address filtering because MAC addresses rarely change. The IP addresses of hosts

Network Switches: Local Network Data Traffic Control

Network switches are computer networks'' building blocks, making up the core of any network setup. In order to understand what they do, it''s important

How to configure port-security on Cisco Switch

Port-security can be used to filter MAC-addresses on Cisco switches. In this lesson you will learn how it works and how to configure it.

What Is a MAC Address, and How Does It Work?

Bluetooth also uses its own MAC address. Related: Wi-Fi vs. Ethernet: How Much Better Is a Wired Connection? How Are MAC Addresses Used? In addition to sending your data to the right

Related Video Reference

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

© 2026 EXF OPTICAL NETWORKS - All rights reserved

Contact Us

Continue your research online:

Website: https://explosivefunctions.co.za
Technical inquiry: https://explosivefunctions.co.za/contact.html
EU project coordination: Parque das Nações, Lisbon, Portugal

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

© 2026 EXF OPTICAL NETWORKS - All rights reserved