Disabling a specific MAC address on a core switch



Overview

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.

Key Takeaways

You can block a specific MAC address on a core switch using port security, MAC lockout, or VLAN access maps depending on your switch model and network setup. Methods to Block a MAC Address1. Port Security (Cisco/Edge-Core/HP switches)Configure the port where the device connects to allow only specific MAC addresses.

Example (Cisco-like syntax):interface GigabitEthernet1/0/1switchport mode accessswitchport port-securityswitchport port-security maximum 1switchport port-security violation shutdownswitchport port-security mac-address This prevents any other MAC addresses from using the port and can drop traffic from the blocked MAC. 2.

MA

C Lockout (HP ProCurve)HP switches support the lockout-mac command to block a MAC address globally.lockout-mac The switch drops all traffic to or from the locked MAC. This is simple but may be bypassed if the device changes its MAC. 3.

MA

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved

C Filtering / VLAN Access Maps (Cisco)Create a MAC access list and apply it to a VLAN to drop traffic from the unwanted MAC:mac access-list extended BLOCK_MACdeny host permit any anyvlan access-map BLOCK_MAP 10match mac address BLOCK_MACaction dropvlan filter BLOCK_MAP vlan-list This method works for dynamically learned MACs and can be applied to multiple VLANs. 4. Centralized Authentication (Optional, Scalable)For larger networks, using 802.

1X with RADIUS or MAB (MAC Authentication Bypass) allows centralized control of allowed MAC addresses. Unknown devices are blocked automatically.

Considerations

Dynamic MA

Cs: Devices with randomized MAC addresses may bypass static blocks. Port vs VLAN: Decide whether to block on a specific port or across a VLAN.

Multiple VLA

Ns: VLAN access maps or centralized authentication are better for multi-VLAN environments. Security Level: Port security is simple but can be circumvented; centralized solutions provide stronger enforcement. By choosing the appropriate method based on your switch model and network design, you can effectively disable or block a specific MAC address on your core switch.

Article Content

Solved: Blocking Certain MAC Addresses

it is possible to allow only certain MAC addresses to connect to the port. However are there any commands which can EXCLUDE some particular MAC address, (without having to follow

How to block specific MAC address in Cisco Switch

(config)# mac address-table static 0349.1245.95ca vlan 192 drop just repeat with as many VLANs that you wanted to deny access for the specific MAC address

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.

Disabling MAC Address Learning on an Interface

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved

For example, if an interface is connected to a server, you can configure a static MAC address entry with the MAC address of the server, disable MAC address learning, and set an action to discard packets

Switch MAC Filtering | Marc''s IT Portfolio

In this Packet Tracer lab, I will be configuring MAC filtering on a switch. In this case, MAC filtering will be used to limit the amount of MAC addresses that can be learned on a single port.

How To Block Mac Address In Juniper Switch

In some scenarios, it may be necessary to block a source-MAC or specific suspicious MAC address from a switch. This can be achieved using firewall filters on the ex series of switches to

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 access to a specific device—but still allow the switch some flexibility in

How to Lock Down Cisco Switch Ports with Port Security (2025 Guide ...

Port Security is a Layer 2 security feature used on Cisco switches to restrict input to an interface by limiting and identifying the MAC addresses of the stations allowed to access the port.

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

Hello. 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

Manage iCloud Private Relay for specific websites, networks, or

Tap Limit IP Address Tracking. Turn off Private Relay for a specific network on your Mac In macOS Ventura or later: Choose Apple menu > System Settings. Click Network in the sidebar, then click the

How to lock the specified MAC address on the port? (port security ...

Check port security. Ping from switch to PC1, PC2, PC3. Capture the packet from PC3. PC3 could receive ARP Request packet from switch, and reply ARP Reply to switch. Since I set the

How to clear Mac-Address on a specific switch''s port

Hi! How to clear MAC-Address on a specific switch''s port Your help is very much appreciated.

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved

Cisco switch mac address block

MAC address security is best if you permit the one or two allowed devices on an interface, usually a PC and a phone. If any other Mac address is detected on that interface the interface will

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

Cisco IOS LAN Switching Command Reference, Release 12.3 T

This chapter presents the Cisco IOS LAN Switching and Multilayer Switching commands. clear mac-address-table To remove a specified address (or set of addresses) from the MAC address table, use

Networking overview | Docker Docs

Published ports When you create or run a container using docker create or docker run, all ports of containers on bridge networks are accessible from the Docker host and other containers connected

M365 Cross-Cloud and Cross-Tenant Collaboration Scenarios

As more of our customers onboard onto our government clouds (GCC, GCC High and DoD) they also need to be able to collaborate across those boundaries. Many cross-cloud scenarios

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,

Related Video Reference

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

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved

Contact Us

Continue your research online:

Website: https://fdsoluciones.es
Technical inquiry: https://fdsoluciones.es/project-enquiry.html

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

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved