MAC Filtering Core Switch



Overview

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.

Key Takeaways

MAC filtering on a core switch allows network administrators to control device access by permitting or denying traffic based on MAC addresses, enhancing network security and preventing unauthorized connections.

Overview of MA

C FilteringMAC filtering is a network access control method where a switch or router allows or blocks devices based on their MAC (Media Access Control) addresses. It can operate in two modes: Allow list mode: Only devices with explicitly approved MAC addresses can access the network. Deny list mode: Devices with specified MAC addresses are blocked, while all others are allowed.

MA

C filtering can be enforced at the port level (device cannot connect) or at the DHCP layer (device connects but cannot obtain an IP address) to prevent unauthorized network usage. Implementation on Core Switches1. Using Port Security (Dynamic MAC Filtering)Port security allows a switch port to learn a limited number of MAC addresses and take action if an unknown device attempts to connect.

© 2026 KENHARDT OPTICAL NETWORKS - All rights reserved

Typical actions include shutting down the port or generating an alert. Example steps: Identify the MAC address of the authorized device. Configure the switch port to allow only that MAC address.

Enable port security and specify the violation action (shutdown, restrict, or protect). Verify configuration using commands like show port-security. 2.

Using MA

C Access Control Lists (Static MAC Filtering)MAC ACLs provide granular control over which devices can send or receive traffic through a switch port. The process involves: Create a MAC ACL specifying permitted MAC addresses and denying all others.

Apply the AC

L to the switch port to enforce the policy. Example configuration on Cisco SG Series switches:permit host 48:bd: 0e: 02:ea: 41 any ace-priority 10permit host 24:b6:fd: 14: 08: 53 any ace-priority 20deny any any ace-priority 40 This allows only the listed MAC addresses and blocks all others. 3.

Integration with VLANsMAC filtering can be combined with VLANs to restrict traffic between network segments. For example, a MAC ACL can be applied to a VLAN interface to control which devices can communicate across VLANs.

Best Practices

Use MA

C filtering as an additional security layer, not the sole protection mechanism. Combine it with strong authentication and encryption. Regularly update allow/deny lists to reflect authorized devices.

Monitor port security violations to detect potential intrusions. For large networks, consider centralized management of MAC ACLs to simplify administration.

Verification

To confirm MAC filtering is active and functioning: Use show port-security to check learned MAC addresses and violation counts. Use show mac access-list to verify ACL rules applied to ports. Test connectivity from authorized and unauthorized devices to ensure enforcement.

By implementing MAC filtering on a core switch, organizations can enhance network security, prevent unauthorized access, and mitigate on-path attacks, while maintaining control over which devices are allowed to communicate on the network.

© 2026 KENHARDT OPTICAL NETWORKS - All rights reserved

Article Content

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.

Solved: MAC filtering

Port security enables you to restrict the number of MAC addresses (termed secure MAC addresses) on a port, allowing you to prevent access by unauthorized MAC addresses.

mac filtering in cisco switch and mac access list

Perhaps filtering inbound and stopping the traffic from traversing your network could work? Here is a support doc that might help with the 3560 mac filtering, using VLAN maps

Cisco | MAC Filtering on SG Series Switches

Learn how to configure MAC address filtering on Cisco SG Series and Small Business switches to enhance network security. Step-by-step instructions and best practices included.

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. Works by keeping an allow list

MAC filtering

MAC filtering is a basic Network Access Control (NAC) method used to control which devices are allowed to connect to a network. It works by checking the MAC address (Media Access Control

How to Configure MAC ACL: Restrict Access and Filter

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

Source MAC address white-list filtering on the PA-220?

What I want to know is it possible (and if so how) to configure a source MAC address white-list filter on the PA-220 so only authorised devices will be able to use the PA-220 as their

© 2026 KENHARDT OPTICAL NETWORKS - All rights reserved

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 mac-filter

How to implement MAC address filtering · Trace Warrior

Set up a MAC allowlist on your router or switch, work around MAC randomization on modern phones, and understand what filtering actually protects

MAC address filtering (on LAN)

MAC filtering is certainly possible on the LAN. For example you can set the switch to only allow one registered MAC address (per port), that way if someone gets near an active port and tries

MAC Filtering: What Is It and Should I Enable It?

MAC address filtering helps protect your network from others. In this article, learn how to enable and disable it to secure your network.

Mac filtering on switches

Hi All, can we filter mac address on specific ports on switches from it learns it dynamically? if yes then how? like switch is getting 10 mac address and I do interested that particular mac address not come

MAC Address Filtering: What It Is and How It Works

Most broadband routers and other wireless access points include an optional feature called MAC address filtering, or hardware address filtering. It improves security by limiting the

Configuring MAC filtering on the switch port using ACL policy

Select the saved policy under MAC ACL and Apply. How to Test: If another machine whose MAC address is not listed in the cache would try to communicate through the switch port.

MAC Address Filtering / Port Security

My question is, for Cisco SG500 switches is there a way for ports to follow MAC address table instead of remembering MAC address per port? I have tried researching online but haven''t got

Mac filtering between switches.

© 2026 KENHARDT OPTICAL NETWORKS - All rights reserved

We have a mac filter on a port of a Cisco 3560. That port connects to the uplink port of a 4-port unmanaged switch. It works great. Today, a different 4-port switch was connected. I would

Port Security/ Mac Filtering

Hello All, Currently I Have all the hosts on my network from multiple VLANS getting IP addresses from the DHCP server, every host has a mac-->ip reservation. This is becoming a

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://kenhardtprimary.co.za
Technical inquiry: https://kenhardtprimary.co.za/project-desk.html
African project coordination: Century City, Cape Town, Western Cape, South Africa

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

© 2026 KENHARDT OPTICAL NETWORKS - All rights reserved