Port restrictions on core switches

AI Overview

Port restrictions on core switches are implemented using port security, which limits the devices that can connect to a port by controlling MAC addresses and defining violation actions.Overview of Port SecurityPort security is a Layer 2 access control feature that allows administrators to restrict which devices can connect to a switch port by specifying allowed MAC addresses and limiting the number of devices per port . This is particularly useful on access ports connecting endpoints like PCs, printers, or IP phones, rather than trunk ports that carry multiple VLANs . Core switches can also use port security to prevent unauthorized access and mitigate attacks such as MAC flooding .Key FeaturesMAC Address Limiting: You can configure a maximum number of MAC addresses per port. If the number of devices exceeds this limit, a security violation occurs .Static and Dynamic MAC Learning: MAC addresses can be assigned statically (manually) or learned dynamically (sticky), allowing the first connected devices to register up to the configured maximum .Violation Actions: When a violation occurs, the switch can respond in three ways:Shutdown: The port goes into an error-disabled state and stops forwarding traffic (default)Restrict: Unallowed traffic is dropped, logging occurs, and SNMP traps can be sentProtect: Unallowed traffic is dropped without logging Configuration ConsiderationsPort security is not supported on EtherChannel interfaces, private VLAN ports, or 802.1X authenticator interfaces .The maximum number of secure MAC addresses is limited by the switch's system capacity and cannot be set below the number of already configured addresses .On core switches, port security is often applied selectively to access ports at the network edge rather than uplinks or trunk ports to avoid disrupting inter-switch traffic .BenefitsPrevents Unauthorized Access: Only authorized devices can connect to the network .Mitigates MAC Flooding Attacks: Limits the number of learned MAC addresses to prevent CAM table overflow .Improves Networ...

Article Content

Security Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst ...

Port-based traffic control is a set of Layer 2 features on the Cisco Catalyst switches used to filter or block packets at the port level in response to specific traffic conditions.

Port Blocking Within a LAN: What It Means and How To Do It Safely

Both matter, and both are regularly mixed up in conversations and policies. I''m going to walk you through what port blocking inside a LAN actually is, why it''s different from ISP port blocking, and how

Core Switch vs. Distribution Switch vs. Access Switch

Core Switch vs. Distribution Switch vs. Access Switch: Understand Their Roles in Ethernet Networks Ethernet networks are growing and becoming more complex,

Core Switch vs. Distribution Switch vs. Access Switch

As the core switches are responsible for routing and switching a high amount of data, the forwarding capacity of the switches must be high. The forwarding capacity of switches is known as the

What Is Port Security on Network Switches?

Learn what port security on network switches is, how it works with MAC address control, and why enterprise switches need it.

Configure Catalyst Switched Port Analyzer (SPAN):

This document describes the recent features of the Switched Port Analyzer (SPAN) that have been implemented.

Configuring Port-Based Traffic Control

Configuring Port-Based Traffic Control Finding Feature Information Your software release may not support all the features documented in this module. For the latest feature information and caveats,

How to configure a port on our core switch for a server

I am looking for some guidance on how to configure a server port on our core switch. For some options, I was thinking this: Option A no switchport no ip address Option B switchport

Internal Firewall vs. ACLs on Core Switches : r/networking

22 votes, 34 comments. Do y''all prefer to setup internal firewalls, pure ACLs on switches, a mix of both with VRFs and route leaking, or a different

How to configure a port on our core switch for a server

If you issue no switch on the interface, the interface will be configured as Layer3 interface and one IP address is expected. With the second option you keep the interface as Layer2 and use

What Is Port Security? How Does Port Security Prevent Attacks

To ensure security of SwitchA and prevent attacks from unauthorized users, configure port security on the ports connecting SwitchA to the endpoints to restrict the number of MAC

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

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.

Restricting Traffic with Isolated Switch Ports

Restricting Traffic with Isolated Switch Ports Last updated May 28, 2026 Save as PDF Table of contents Configuration Implementation and Best

Differences Between the Core Switch and Normal

The so-called core switch is for the network architecture. If it is a small local area network with several computers, a small switch with 8 ports can

Understand Port Group Restrictions on C9500X and

On the C9500X-60L4D switch, and on the C9600-LC-48YL and C9600-LC-40YL4CD linecards, when used with the C9600X-SUP-2; there is a

Mastering Switch Port Configuration: Avoiding Common Pitfalls in ...

Optimize enterprise switch deployments by mastering port configuration. Learn to prevent speed mismatches, VLAN errors, PoE issues, and LACP failures for seamless network performance.

Switchport Port Security Explained With Examples

This tutorial explained the commands and configuration steps you need to secure switch ports. Learning these commands and configuration steps allows you to secure your network from

Azure OpenAI Service Multitenant Load Balancing and

This example shows how a multitenant service can distribute requests evenly among multiple Azure OpenAI Service instances and manage tokens per minute

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE ...

VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN

BW restriction/control on switch port(access port)

Hi, Core sw (vlan10) == Etherchannel== Access (Vlan10)Gi0/1 === Server (vlan 10). Access sw = 2960 I need to restrict the BW on switch port where my server connected (gi0/1). I have

FS Community

Hier sollte eine Beschreibung angezeigt werden, diese Seite lässt dies jedoch nicht zu.

How to Secure Switch Ports Using the Cisco Port

Although the most secure option for dealing with unused switch ports is to just disable them, this does nothing to secure in-use ports. And in a live

Security Configuration Guide, Cisco IOS XE 17.18.x (Catalyst 9600 Switches)

This chapter provides configuration information about port-based traffic control.

Port Security on Switches | Shutdown | Protect | Restrict ⋆ CCNA

We will learn Switch Port Security, how to configure port security on Cisco switches, violation modes: Shutdown, Protect, Restrict

SAP Help Portal | SAP Online Help

SAP Help Portal provides online help and support for SAP software users.

Restricting Traffic with Isolated Switch Ports

In the example below, switch A''s uplink port has been isolated, so clients connected to any other isolated port on A are unable to communicate with

Ports restriction

Hi, We need to restrict Layer 2 switch ports for blocking another switch connection. Can any body guide me how to perform this task. Regards, Faisal

What is Cisco Port Security? | Definition, Types & Modes!

Learn precisely what Cisco Port Security is and what its features are in our simple guide. Understand Switch restriction logic!

Ethernet Switch: Port speed limits stop single devices hogging

This article will provide an in-depth analysis of the technical principles and practical techniques of Ethernet switch port speed limiting to help enterprises build stable and efficient

Contact Us

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

Website: https://energy-powertools.eu
Email: info@energy-powertools.eu
Phone: +49 172 6389472
Address: Musterstraße 12, 10115 Berlin, Germany

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