

Switch Port Access Restrictions



Overview

Port Security If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempt.

Key Takeaways

Port security allows you to restrict which devices can connect to a switch port by limiting MAC addresses and defining violation actions. What is Port SecurityPort security is a Layer 2 access control feature on switches that restricts which devices can connect to a specific port. It works by limiting the number of MAC addresses allowed on a port and specifying which MAC addresses are permitted, either statically or dynamically.

This prevents unauthorized devices from accessing the network and mitigates attacks like MAC flooding.

Key Features

Limit MA

C addresses per port: You can set a maximum number of devices that can connect to a port, typically up to 132 on Cisco switches. Allow specific MAC addresses: You can configure MAC addresses statically (manually) or dynamically (sticky learning) to control which devices are allowed. Violation actions: When an unauthorized device attempts to connect, the switch can respond in three ways: Shutdown: The port is disabled and stops forwarding traffic (default behavior).

Restrict: The port remains active, drops unauthorized traffic, and logs the violation.
 Protect: The port remains active, drops unauthorized traffic, but does not log the violation.
 Configuration Steps on Cisco Switches
 Enter interface configuration mode for the port you want to secure: `CodeCopySwitch# configure terminal`
`Switch(config)# interface FastEthernet0/1` Set the port to access mode (required for port security):
`CodeCopySwitch(config-if)# switchport mode access` Enable port security:
`CodeCopySwitch(config-if)# switchport port-security` Set the maximum number of allowed MAC addresses:
`CodeCopySwitch(config-if)# switchport port-security maximum 2` Specify allowed MAC addresses (optional): Static: `CodeCopySwitch(config-if)# switchport port-security mac-address 0001.`

0203. 0405 Dynamic (sticky): `CodeCopySwitch(config-if)# switchport port-security mac-address sticky` Define the violation action: `CodeCopySwitch(config-if)# switchport port-security violation restrict` Use Cases
 Lock a wall jack to a single device to prevent rogue access points or unauthorized switches. Secure printers, cameras, or IoT devices by pinning their MAC addresses.

Prevent MA

C flooding attacks by limiting the number of learned MAC addresses. Properly implementing port security ensures that only authorized devices can access the network, improves visibility of connected devices, and enforces organizational security policies at the access layer.

Article Content

Port Security

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified

Configuring Port Security

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified

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

Switch Port Security is the security mechanism used in switches. With this mechanism, a specific port of a switch can be protected with undesirable access. Here, we will learn the theory of this lesson. We

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.

What is Switchport Mode Access? How to Configure Switchport Mode

Switch ports can be set either in trunk or access mode to have more control on switch port behaviour. Using switchport access mode forces the port to be an access port and when any device

Restricting Traffic with Isolated Switch Ports

When ports on a switch have been isolated, the MS will not send from one isolated port to another. This can be useful in a multi-tenant environment, for example, where clients should be

Ethernet Switch Port Types Explained 2026: RJ45,

Intro Ethernet switch port types define the performance, scalability, and architecture of modern networks. RJ45 ports serve access-layer copper

Port access policy

Port access policy allows network administrators to define a set of rules. These rules are used to restrict or alter the passage of traffic for clients onboarding to a switch that has port security (802.1X, MAC

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.

How To Manage and Secure Network Switch Port Access

Learn effective strategies to manage and secure network switch port access, reducing risks and strengthening your network security posture.

How to Lock Down Cisco Switch Ports with Port

Today I'm breaking down a simple yet powerful security mechanism every network admin should understand — Port Security on Cisco switches.

Introduction to Switch Port Security

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

BW restriction/control on switch port(access port)

I need to restrict the BW on switch port where my server connected (gi0/1). I have to restrict my port utilization to 80% as my server pumping huge data on port Gi0/1 and it should not

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

How to Configure a Cisco Switch (step by step)

If you're looking to configure a switch for the first time, this post is for you. Learn step-by-step configuration commands for Cisco IOS Switches.

Solved: Hub/Switch

Solved: Hi How do I restrict helpdesk or users from plugging hub or switch on the network. If Hub/Switch is connected to the switchport then port turn down or disable. What are other

Configuring Port Security on Cisco IOS Switch

This security feature of Cisco IOS Switches can only be configured on access ports and by default, this feature is disabled. Enabling Port Security on Cisco Switch :

Port Access Control

Is there a way to limit a users access on the network by programming a port on a Cisco switch to shutdown at a certain time and enable at a certain time?

Contact Us

Continue your research online:

Website: <https://artduferoger.fr>

Technical inquiry: <https://artduferoger.fr/contact.html>

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

