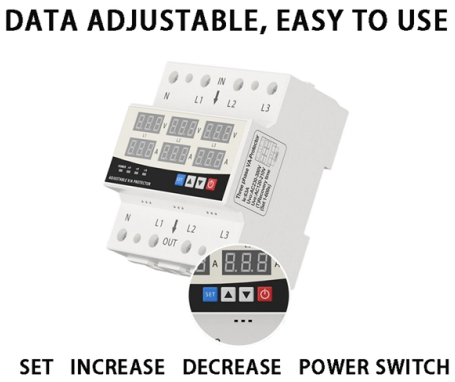
Switch access IP restricted



Overview

This chapter provides configuration information about controlling switch access with passwords and privilege levels.

Key Takeaways

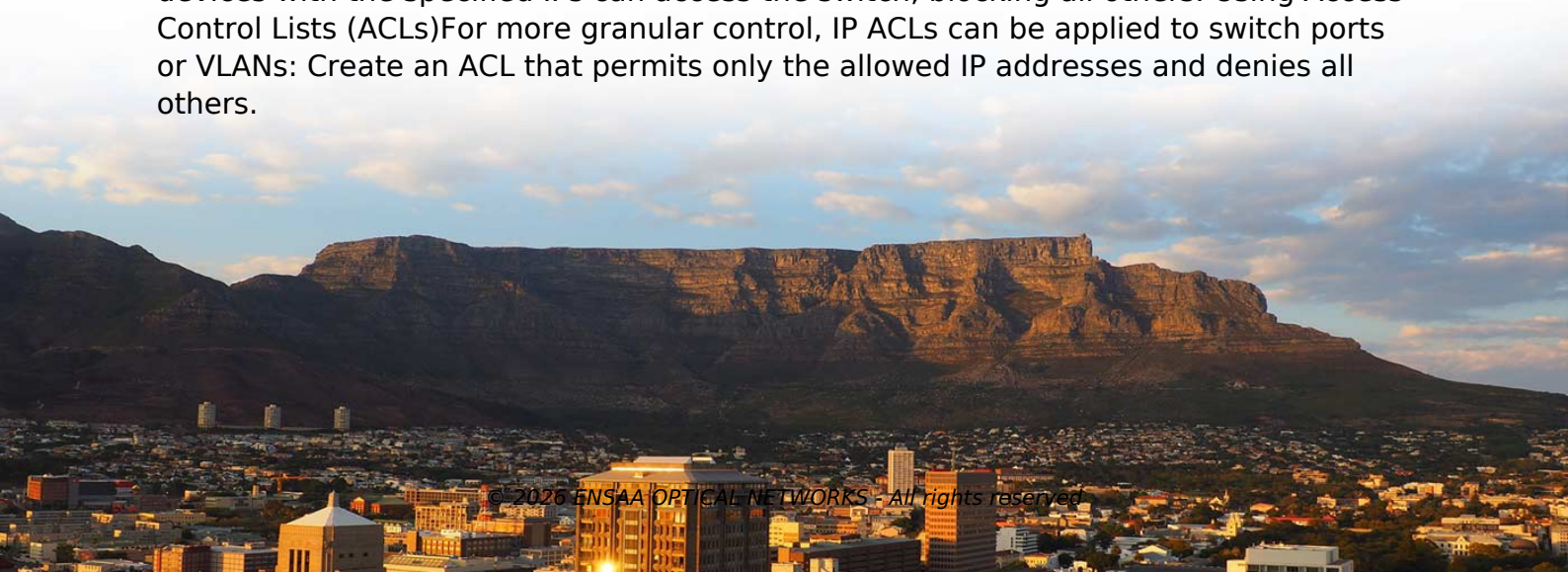
You can restrict access to a switch by configuring IP-based access control or ACLs, allowing only specific IP addresses to manage or communicate through the switch. IP-Based Access ControlMany managed switches support IP-based access control, which allows you to specify which IP addresses can access the switch management interface (HTTP, HTTPS, SSH, Telnet) or network services. To configure this: Enable Access Control in the switch's security settings.

Select IP-based mode from the control options. Specify allowed IP addresses and subnet masks. For example, to allow only a single IP, use a mask of 255.

255. 255. 255; for a subnet, use the appropriate subnet mask (e.g., 192.

168. 1. 0/24).

Apply the configuration to the desired management interfaces. This ensures that only devices with the specified IPs can access the switch, blocking all others. Using Access Control Lists (ACLs)For more granular control, IP ACLs can be applied to switch ports or VLANs: Create an ACL that permits only the allowed IP addresses and denies all others.



© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

Apply the AC

L inbound on the switch port or VLAN interface. On Cisco switches, this can be done using extended ACLs, e.g., ip access-list extended 102 followed by permit and deny rules for specific IP ranges.

AC

Ls can also restrict traffic to specific services, such as HTTP, HTTPS, or SSH, providing additional security.

VLA

N Isolation and Layer 3 ConsiderationsAnother approach is to assign the allowed device to a dedicated VLAN: The VLAN can be isolated from other network segments. Only the allowed IP within that VLAN can communicate with the gateway or management interface. This method works well in combination with ACLs for Layer 2 switches, while Layer 3 switches can enforce IP ACLs directly.

Additional Security MeasuresMAC-based access control can complement IP restrictions to prevent IP spoofing.

RADIU

S or TACACS+ authentication can provide centralized access control for larger networks. Privilege levels and passwords should be configured to limit command access on the switch. By combining IP-based access control, ACLs, VLAN isolation, and proper authentication, you can effectively restrict switch access to only authorized IP addresses, enhancing network security.

Article Content

Understanding Network Access Controls & Your Switch

When your Nintendo Switch appears to be "paused" or experiencing connectivity issues, it is often due to wireless network access controls enabled by your internet service provider (ISP)

Cisco IE3500 Series Switch Software Configuration Guide, Cisco IOS

This chapter provides configuration information about controlling switch access with passwords and privilege levels.

Solved: Access list to restrict certain IPs

Allow all machines that has a valid IP i.e any IP from 192.168.1.101 to 192.168.1.150 to connect to the cisco router and consequently access the Internet. Thus a machine with an IP such a

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

Restrict Access to Cisco Switch Based on IP Address

In this article, I''ll walk you through the steps to configure access profiles and profiles rules for your Cisco switch. Note: The following method I am going to describe also allows you to restrict

SNMPv3 access to the switch

If you want to restrict access to one or more specific nodes, you can use the IP Authorized Manager feature for the switch. (See the access security guide for your switch.)

only permit specific ip address on a switch port

What you need is a DHCP server that assigns predefined IP addresses based on the MAC address. Therefore it doesn''t matter on which port of the switch the client connects. If security is

What Is the Default Username and Password for Cisco Switches?

Learn the default Cisco switch username and password. Discover which models use “cisco/cisco,” why most have no defaults, and how to secure login access

Switch ACLs: how to config ACL to permit internet access but restrict ...

We have some devices (security cameras, security keypads, backup/archival servers) that need to have internet access (IoT-style dashboards, updates, etc) but I need to restrict access to

How to Change/View Existing Internet Connection Settings on

In this article, you''ll learn how to change the settings of a registered network (including wireless security, IP address, DNS, Proxy, MTU, etc.) on Nintendo Switch 2 and Nintendo Switch.

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

How to configure Access Control to block users'' access to the switch ...

You can configure Access Control to allow only specific users to access the switch and block the others. Access Control can work in three modes: IP-based Mode, MAC-based Mode and

only permit specific ip address on a switch port

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

Hi all, couldnt find a solution yet, so will be happy for your assisstance. Usually I use switches vlans and bandwidth management purposes. I''m looking for a solution to only permit a

Set Up Access Restrictions

When you set up access restrictions, you can define a priority-ordered allow/deny list that controls network access to your app. The list can include IP addresses or Azure Virtual Network

Restrict port to specific range of IP addresses?

All my access switches are 2960X, and I''d like to restrict all the ports to only allow IP addresses in a specific range to connect to the port. I want this to insure only IPs in the client range

Fortifying Your Network: A Comprehensive Guide to Restricted SNMP ...

However, unrestricted SNMP access creates a security vulnerability. This blog equips you with the knowledge and configuration examples to implement robust restricted SNMP access on your

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

Solved: Restrict Internet Access

Hi, I have a radio link from my office to another location. This radio link is connected to an access switch at my office. They are on the same Vlan. I''m tryin to look for a way to restrict them

Managing User Configuration, Cisco Catalyst PON Series Switches

Overview of IP Limit Configure IP Limit Monitor IP Limit Configuration Example: Configuring IP Limit Overview of IP Limit By default, there is no restriction on the user IP addresses

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

Contact Us

Continue your research online:

Website: https://ensaa.es
Technical inquiry: https://ensaa.es/contact.html

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

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved