Switch Port Access Control



Overview

Port-Based Access Control (802. 1X) provides switch-level security that allows LAN access only to users who enter the authorized RADIUS username and password on 802. 1X-capable clients (sup-plicants). This chapter describes how to configure IEEE 802. Unless otherwise noted, the term switch refers to a standalone switch or a switch stack. Switchports are always. Cisco Meraki MS switches offer the ability to configure access policies, which require connecting devices to authenticate against a RADIUS server before they are granted network access. These access policies are typically applied to ports on access-layer switches to prevent unauthorized devices. Local area networks are often deployed in a way that allows unauthorized clients to attach to network devices, or allows unauthorized users to get access to unattended clients on a network. To resolve security issues on wireless LANs (WLANs), the IEEE 802 committee proposed. This section outlines the steps for configuring 802. On the ports you will use as authenticators, either. Access control lets you define rules to filter incoming and outgoing packets based on IPv4, IPv6, and MAC addresses. Each access control list (ACL) contains up to 16 access control entries (ACEs).

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved

Article Content

Configuring IEEE 802.1x Port-Based Authentication

You can configure a restricted VLAN (also referred to as an authentication failed VLAN) for each IEEE 802.1x port on a switch stack or a switch to provide limited services to clients that cannot access the

MS Switch Access Policies (802.1X)

This article outlines options available for access policies, how to configure access policies in the Meraki dashboard, and the configuration

Configuring Port-Based Access Control (802.1X)

Port-Based Access Control (802.1X) provides switch-level security that allows LAN access only to users who enter the authorized RADIUS username and password on 802.1X-capable clients (sup-plicants).

802.1X Authentication: A Port-based Network Access

Explain the basic concepts and working principles of 802.1X, analyze the integration of switch and 802.1X, changes in port status, and dynamic

Configuring Switch Ports as 802.1X Authenticators

Enable 802.1X user-based or port-based authentication on the individual ports you want to serve as authenticators. On the ports you will use as authenticators, either accept the default 802.1X settings

Access control

ACLs provide basic security for network access by controlling whether packets are forwarded or blocked at the switch ports. They also provide

802.1X: Port-Based Network Access Control

Port-based network access control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service,

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.

Network security deploying 802.1X & NAC on switches

This article delves into how deploying 802.1X on switches significantly bolsters network security by authenticating and authorizing devices

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved

LANCOM Whitepaper Switch security with IEEE 802.1X

Port-based IEEE 802.1X regulates the authentication of clients at the switch ports by verifying certificates or access credentials against a RADIUS server. After success-ful authentication, the port

Assign Azure roles using the Azure portal

Learn how to grant access to Azure resources for users, groups, service principals, or managed identities using the Azure portal and Azure role-based access control (Azure RBAC).

Configuring IEEE 802.1x Port-Based Authentication

Overview of IEEE 802.1x Port-Based Authentication The 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a

Complete Cisco Commands Cheat Sheet for Devices

Use our essential Cisco commands cheat sheet for quicker and easier device configuration and management. Download the free cheat sheet here.

Cybersecurity-Networking-Security/README.md at main · Ruffy101 ...

Access control lists was implemented to regulate traffic flow and enforce network security policies. Extended ACLs were used to provide granular control based on source, destination, protocol, and port.

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?

Access Control on the Wired Network

Access Control on the Wired Network This workflow describes a phased approach to deploy IEEE 802.1x port-based authentication to provide secure and identity-based access control at the edge of

What is Access Port in Switch?

Learn exactly what the Access port is, which we often hear about in switch network devices. Discover how to set up these ports in your LAN!

DwyerOmega | Shop for Sensing, Monitoring and

Explore DwyerOmega''s comprehensive range of industrial sensing, monitoring, and control solutions from thermocouples to pressure transducers engineered for

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved

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://dolphinspreschool.co.za
Technical inquiry: https://dolphinspreschool.co.za/project-desk.html
African project coordination: Waterfall City, Midrand, Gauteng, South Africa

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

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved