

Switch access authentication configuration failed



Overview

Troubleshoot Dot1x on Catalyst 9000 Series Switches This document describes how to configure, validate and troubleshoot 802.1x network access control (NAC).

Key Takeaways

Authentication failures on switches often result from misconfigured AAA method lists, incorrect domain settings, or improper ordering of local and server-based authentication methods. Common Causes of Authentication FailuresAAA Method List Misconfiguration Switches use a method list to determine the order of authentication attempts. If the first method fails to respond, the switch tries the next method.

However, if a server responds with a denial, the process stops and no other methods are attempted. For example, if TACACS+ is listed first and denies a user, the local database will not be checked unless explicitly configured as a backup.

Incorrect Domain or NA

C Mode On some switches, AAA configurations are domain-based. Users must belong to the correct domain, and the domain must have proper AAA settings. Unified mode prioritizes domains in the username, default domains, and global default domains.



Misalignment between user domain and AAA configuration can cause authentication failures. Authorization vs Authentication Issues Even if authentication succeeds, authorization may fail if the switch cannot map the user to the correct privileges or network resources. Common causes include misconfigured downloadable ACLs (dACLs) or incorrect AAA authorization commands, such as using local instead of radius in the authorization group.

Platform or IOS Version Differences AA

A behavior can vary between switch models and IOS versions. A configuration that works on one platform may fail on another, especially regarding local vs server-based authentication precedence.

Recommended Troubleshooting Steps

Verify Method List Order Ensure the AAA method list is correctly ordered. For example, to allow local users as a backup to TACACS+, configure: `CodeCopyaaa authentication login default group tacacs+ local` This ensures the switch checks TACACS+ first, then the local database if the server is unavailable.

Check Domain and NA

C Mode Run commands like `display authentication mode (Huawei)` or equivalent to verify NAC mode and domain assignment. Confirm that the user belongs to a domain with correct AAA settings. Validate Authorization Configuration Ensure the authorization method matches the authentication method.

For example, on Cisco switches, use: `CodeCopyaaa authorization network default group radius` instead of local if RADIUS is intended for network access. Test Connectivity to Authentication Servers Verify that RADIUS or TACACS+ servers are reachable and responding. Check logs for denied attempts or misconfigured credentials.

Review Logs and Debug Output Use commands like `show running-config | section aaa` and server logs to identify whether authentication or authorization is failing and why.

Best Practices

Always configure backup authentication methods to prevent lockouts. Keep local accounts for emergency access. Ensure consistent AAA configuration across all switches in the network.

Regularly test authentication and authorization after configuration changes. By carefully reviewing method lists, domain assignments, and authorization settings, most switch access authentication failures can be resolved.

Article Content

Troubleshoot Dot1x on Catalyst 9000 Series Switches

This document describes how to configure, validate and troubleshoot 802.1x network access control (NAC) on Catalyst 9000 series switches.

Authorization Failed Cisco Switch: Common Headache? Could

This isn't just about inconvenience; a single authorization failed scenario on a core Cisco switch during a crisis can stall recovery efforts, escalate downtime costs dramatically, ...

Troubleshooting 802.1X Authentication Failures

If the authentication method configured on the switch is inconsistent with that on the client or RADIUS server, run the dot1x authentication-method { chap | pap | eap } command in the 802.1X access

MS Switch Access Policies (802.1X)

By configuring a Failed-authentication GPACL or SGT, you can control and restrict the network resources accessible to devices that do not successfully authenticate, such as limiting

Authenticating

To access the new capabilities like configuring multiple authenticators, setting multiple audiences for an issuer, switch to using the configuration file. To use structured authentication,

Common Causes for Access Authentication Failures

After Portal Authentication Is Successful, the Authentication Page Is Still Displayed When Users Access the Network (Unexpected Disconnection of Portal Authentication Users)

Port access 802.1X authentication debugging and troubleshooting

An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

cisco ios

In your case, the device will use the TACACS database. It will use the local database ONLY if TACACS is unavailable. If TACACS doesn't have the user in the database, it will issue a "Reject" message,

Configuring the switch authentication method

The authorized privilege level (operator or manager) is returned to the switch by the TACACS+ server. Default: Single login disabled. Selects the type of security access: local

VMware Cloud Foundation (VCF) Blog - Home Page

VMware Cloud Foundation (VCF) - The simplest path to hybrid cloud that delivers consistent, secure and agile cloud infrastructure. Read more.

OpenVPN Connect

Web authentication for SAML SSO support HTTP proxy configuration Seamless split-tunneling and auto-reconnect Works over Wi-Fi, LTE/4G, 5G, and all mobile networks Easy setup & import of .ovpn

Viva Learning feature announcements at Ignite 2023 | Microsoft ...

Learn more about this feature from our documentation page. This feature requires a Viva Learning or Viva Suite license to access. Advanced language configuration This feature allows

Microsoft Entra releases and announcements

Learn what is new with Microsoft Entra, such as the latest release notes, known issues, bug fixes, deprecated functionality, and upcoming changes.

Advanced setup

If this fails with command not found or another error, see Troubleshoot installation and login. For a more detailed check of your installation and configuration, run claude doctor: ... Claude Code requires a

OneUptime | The Open-Source Observability Platform

Catch outages in seconds, page the right engineer, and keep customers in the loop — one open-source platform that replaces your monitoring, incident management, and status page stack.

Microsoft Options to Migrate SQL Server Databases | Microsoft

Restrict access to the obfuscation configuration, logs, and any intermediate exports that may contain raw values. Verify effectiveness: Add validation steps to confirm that sensitive values

How to fix the error "AADSTS50076: Due to a

However, I get this error: "AADSTS50076: Due to a configuration change made by your administrator, or because you moved to a new location, you must use multi

Solved: I am unable to login to the switch using TACACS+ login after ...

The switch kept going in cycles showing the banner and then giving the authentication failed message 3 times and the cycle starts with the banner and authentication failed message i

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://metramarket.es>

Technical inquiry: <https://metramarket.es/contact.html>

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

