Core switch ports under attack



Overview

Core switch ports aggregate traffic from multiple access switches, so port security isn't appropriate. Instead, stability and resilience come from trunking, root guard, storm control, and strong physical access controls., Cisco Nexus, Arista) act as the data center's highway, using protocols like BGP, OSPF, or VXLAN to move traffic between aggregation layers. Attackers who compromise a core switch can sniff, redirect, or drop all inter-rack traffic. Therefore, control plane policing (CoPP) and. Cyber attacks are intentional attempts to infiltrate or disrupt computer networks, systems, or devices, often through a switch that connects various pieces of the network infrastructure. Locking them down with port security (one MAC per port), BPDU Guard, and VLAN segmentation helps prevent rogue devices, hubs, and accidental loops. Core switches are secured differently Core switch ports aggregate traffic from multiple access switches, so. Router 1 has port 1/0/1, this goes to core switch port 0/48 Router 2 has port 1/0/1, this goes to core switch port 1/47 Core switch port 0/1 goes to 1 firewall and port 1/1 goes to 2 firewall Core switch port 0/2 goes to 2 firewall and port 1/2 goes to 1 firewall 0/48 is tagged VLAN 100 which has. Infected LAN-switch takes unusual actions which sends load of informational messages to continuously be shutting down its interfaces. Which makes the vulnerability of interfaces of the LAN-switch and launch an. We use switches to reduce the number of packet collisions. This chapter covers two common attacks against a switch.



© 2026 METRA FIBER MARKET - All rights reserved

Article Content

Data Center Under Siege: How Your Packets Survive Firewalls, Core ...

Attackers who compromise a core switch can sniff, redirect, or drop all inter-rack traffic. Therefore, control plane policing (CoPP) and secure management (SSHv2, SNMPv3) are mandatory.

Network Attacks Unveiled: Understanding the Threats to Your Switches

Cyber attacks are intentional attempts to infiltrate or disrupt computer networks, systems, or devices, often through a switch that connects various pieces of the network infrastructure. The

Access vs Core: Where Network Security Really Matters

On access switches, unused ports should be placed in an unused VLAN and shut down. On core switches, unused ports are administratively shutdown and documented for future growth.

Switch can be attacked if not behind a firewall

If your router is compromised, an attacker can pivot to your core switch without ever going through a firewall. What you''re saying is the switches aren''t directly exposed to the internet, which is also true,

Implementing PortSecurity to Switchports to avoid vulnerability

Best practice to avoid such attack that must implement port-security on switchports, restricting devices that can use the port only authorized MAC addresses in end point of LAN-switch.

Man-in-the-Middle (MITM) – Switch Hacking – Mastering Enterprise ...

Each physical port on a switch creates an isolated packet collision domain. This chapter covers two common attacks against a switch. Our GNS3 test environment is not designed to withstand this

8 Ways to Cyber-Harden Ethernet Switches

Ethernet switches have long served as the cornerstone of communication networks. Because of their widespread deployment, they are an ideal attack surface for cybercriminals.

Hacking Layer 2: Fun with Ethernet Switches

¥ A station can spoof as a switch with ISL or 802.1Q signaling (DTP signaling is usually required as well, or a rogue DTP speaking switch) ¥ The station is then member of all VLANs ¥ Requires a trunking

© 2026 METRA FIBER MARKET - All rights reserved

How Switch Port Security Can Save You from Cyber Attacks

Discover how switch port security can protect your network from cyber attacks, prevent unauthorized access, and keep your data safe!

How Insecure Network Devices Can Expose Data Centers to Attack

Although data center networking hardware, like switches, tends to receive less attention than servers during discussions of cybersecurity, the reality is that network equipment can pose just

Network Switch Security 101 | ServerMania

Implementing strong switch security is crucial to protect networks from unauthorized access and potential attacks. Enable port security features, implement port security, and configure

Direct To Video (DTV) Films: The Good And The Bad

Most of the films below have had limited theatrical release, have gone straight to Video On Demand (VOD) or have gone Direct to Video (DTV). There is a lot of good and bad stuff out there, some of

Man-in-the-Middle (MITM) – Switch Hacking – Mastering Enterprise ...

We use switches to reduce the number of packet collisions. Each physical port on a switch creates an isolated packet collision domain. This chapter covers two common attacks against a switch. Our

Switch can be attacked if not behind a firewall

The auditor is valid in raising this, because the switch being attacked is a core switch and so even if the attack surface is minimal, the impact is large. I''ll be buying 2 x switches that are "outside" my normal

Implementing Port Security to Mitigate Network Attacks

Learn how implementing port security enhances network protection by preventing unauthorized access, rogue devices, and switch security breaches effectively.

Basic Switch Security Concepts Explained

There are various techniques to enhance switch port security, including: Secure Unused Ports: Disable unused switch ports to prevent unauthorized devices from connecting to the network.

Evaluation on Security Risks of the Switch Module on the Network ...

© 2026 METRA FIBER MARKET - All rights reserved

Based on network security threats and switch module vulnerabilities, you can evaluate security risks encountered by the switch module and provide suggestions on suppressing security

Ports are getting smarter and more hackable

State-linked cyber attacks on maritime port infrastructure are up, exposing critical vulnerabilities in trade, military logistics systems.

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.

© 2026 METRA FIBER MARKET - All rights reserved