

Article Overview

A typical access switch configuration includes VLAN assignment, interface setup, user authentication (802.1X, MAC, or portal), and basic management security to control network access and ensure connectivity.

VLAN and Interface Configuration

Access switches are usually configured to segment the network using VLANs. Each interface connecting to end devices is typically set as an access port and assigned to a specific VLAN based on department or user group requirements. For example, VLAN 10 may be assigned to employees, while VLAN 20 is used for servers or management traffic. Interfaces connecting to authentication servers or uplinks are also assigned to appropriate VLANs to ensure proper communication ().

Authentication and Access Control

To secure network access, access switches often implement Network Access Control (NAC) using multiple authentication methods:

- o 802.1X Authentication: Provides secure port-based access control, requiring client software on user devices. It is typically prioritized for employees ().
- o MAC Address Authentication: Allows devices without 802.1X clients to authenticate based on registered MAC addresses.
- o Portal (Web) Authentication: Used for guests or devices that move frequently; users log in via a web portal before gaining network access (). These methods can be deployed concurrently, with the switch configured to apply authentication in a defined sequence. AAA (Authentication, Authorization, and Accounting) schemes and RADIUS server templates are commonly used to manage authentication and assign network rights ().

Basic Switch Management

Access switches require secure management configuration:

- o Hostname and Device Identification: Assign a descriptive hostname for easier management.
- o Console and VTY Lines: Configure passwords for console and virtual terminal (VTY) access to prevent unauthorized login ().
- o DHCP and IP Settings: Enable DHCP if the switch provides IP addresses to clients or configure static IPs for management.
- o Interface Security: Limit the number of MAC addresses per port, enable port security, and configure ARP detection to prevent spoofing ().



Typical Configuration of Access Switches

Policy and Segmentation

Modern enterprise networks often integrate identity-based policies:

- o Cisco SD-Access uses Security Group Tags (SGTs) to enforce micro-segmentation and group-based policies.
- o Policies are applied dynamically based on user or device identity, simplifying access control and improving security ().

Example Workflow

- o Create VLANs and assign interfaces to VLANs.
- o Configure AAA and RADIUS server templates.
- o Enable 802.1X, MAC, and portal authentication as needed.
- o Set interface access mode and maximum number of users.
- o Configure console and VTY passwords for management.
- o Apply security policies and verify connectivity. This configuration ensures that authorized users gain appropriate network access, devices are segmented by VLAN, and management access is secured, forming a standard blueprint for enterprise access switch deployment ().

Meanwhile, core switches start in the gigabit range and go up quickly. Core switches are typically fiber

Discover how to optimize network performance and security with Switch Port Configuration, covering Access, Hybrid,

Configuring a Cisco switch is a fundamental task for network administrators, as it lays the groundwork for efficient and

Don't overspend on network hardware. Our expert guide explains core, distribution, and access switches so you can

st access switch is a common configuration. This approach extends the local LAN access ports in the workspace in order to allow a

Fixed Configuration Switches typically come in 5, 8, 10, 16, 24, 28, 48, and 52-port configurations. These ports may be

All that's left is to test your access, reload the switch, and ready the cables. Once that's done, label your

switch, rack it up, and go

Core Switch vs Access Switch The core switch is used in the center of your network, while an access switch is placed

Follow these simple best practices to set up a new network switch. Still fuzzy? Just like riding a bicycle, nobody's born knowing how

Learn about the different types of network switches, including managed, unmanaged and Power over Ethernet

Unlike other lower class switch vendors (which are plug-and-play), the Cisco switch needs some initial basic configuration in order to

Whether the configuration deployment of a switch is completed all at once or done in phases, the basic switch settings must first be

A multinational bank might have core switches in regional data centers, distribution switches in each country office, and

5) The typical web interface displays below. You can view the switch's running status and configure the switch on this interface.

Cisco switch configuration guide. Step-by-step setup instructions for efficient network performance.

Learn what an access switch is, how it works at the network edge, why PoE and port density matter, and how Wi-Fi 7

Web: <https://bssoda.pl>

