GENERAL

cisco 3560 configuration guide

Published: September 3, 2026 | Index ID: #-

Introduction

When you first power up a Cisco Catalyst 3560 switch, you're staring at a powerful, stackable device that can support a wide range of enterprise networking needs. Whether you're building a campus network, a data center spine, or a branch office, the Cisco 3560's versatility makes it a popular choice for many IT professionals. However, to unlock its full potential, you must go beyond the factory defaults and dive into a comprehensive **cisco 3560 configuration guide**. This guide will walk you through every step—from initial setup to advanced features—so you can configure the switch securely, efficiently, and reliably.

Why the Cisco 3560 Is Still Relevant

Although newer Catalyst models are available, the Cisco 3560 remains relevant for several reasons:

- Stacking Capability – The 3560 supports up to 8 switches in a single stack, providing a single logical device with increased port density and redundancy.
- Layer 3 Routing – Built in IP routing allows the switch to perform routing tasks without a separate router.
- Advanced Features – Features such as QoS, port security, and IEEE 802.1X authentication are fully supported.
- Proven Reliability – Many enterprises still rely on 3560 stacks for mission critical services.

Because of these strengths, a solid **cisco 3560 configuration guide**is essential for network engineers who need to maintain, upgrade, or integrate these switches into modern infrastructures.

Prerequisites Before You Begin

Before you start configuring, make sure you have the following:

1. Access to a console port (RJ 45 or USB, depending on the model).
2. An appropriate console cable and terminal emulation software (PuTTY, Tera Term, SecureCRT).
3. Basic knowledge of Cisco IOS command syntax.
4. IP address of the management interface or a DHCP enabled network.
5. Documentation of your network design, including VLAN IDs, IP subnets, and port assignments.

Having these items ready will help you avoid common pitfalls and ensure a smooth configuration process.

Initial Setup: The First Steps

Connecting to the Console

Use a serial-to-USB adapter if your PC lacks a serial port. Open your terminal emulator and configure the following settings: 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

Entering Global Configuration Mode

Once you're connected, you'll see the Switch> prompt. Type enable to enter privileged EXEC mode, then configure terminal to access global configuration mode. The prompt should change to Switch(config)#.

Setting a Hostname and Domain

Assign a meaningful hostname to identify the switch within your network:

```
Switch(config)# hostname BranchSwitch
BranchSwitch(config)# ip domain-name branch.example.com
```

Creating an Administrator Password

Secure the device by setting a privileged EXEC password:

```
BranchSwitch(config)# enable secret StrongPassword123
```

Use a strong, unique password to protect against unauthorized access.

Basic Interface Configuration

Configuring the Management Interface

The 3560's Ethernet0/1 port can be used as a management interface. Assign an IP address and subnet mask:

```
BranchSwitch(config)# interface Ethernet0/1
BranchSwitch(config-if)# ip address 192.168.10.10 255.255.255.0
BranchSwitch(config-if)# no shutdown
BranchSwitch(config-if)# exit
```

Verify connectivity with ping 192.168.10.1 to the gateway.

Enabling SSH for Secure Remote Access

To replace telnet with SSH, generate RSA keys and enable the SSH server:

```
BranchSwitch(config)# crypto key generate rsa
BranchSwitch(config)# ip ssh version 2
BranchSwitch(config)# line vty 0 15
BranchSwitch(config-line)# transport input ssh
BranchSwitch(config-line)# login local
BranchSwitch(config-line)# exit
```

Now you can connect via SSH from a remote terminal.

VLAN Configuration and Trunking

Creating VLANs

Define VLANs required for your network:

```
BranchSwitch(config)# vlan 10
BranchSwitch(config-vlan)# name Sales
BranchSwitch(config-vlan)# exit
BranchSwitch(config)# vlan 20
BranchSwitch(config-vlan)# name Engineering
BranchSwitch(config-vlan)# exit
```

Assigning Ports to VLANs

Configure access ports for each VLAN:

```
BranchSwitch(config)# interface range Ethernet0/2 - 4
BranchSwitch(config-if-range)# switchport mode access
BranchSwitch(config-if-range)# switchport access vlan 10
BranchSwitch(config-if-range)# exit
BranchSwitch(config)# interface range Ethernet0/5 - 7
BranchSwitch(config-if-range)# switchport mode access
BranchSwitch(config-if-range)# switchport access vlan 20
BranchSwitch(config-if-range)# exit
```

Setting Up Trunk Links

When connecting to another switch or a router, use a trunk port:

```
BranchSwitch(config)# interface Ethernet0/24
BranchSwitch(config-if)# switchport mode trunk
BranchSwitch(config-if)# switchport trunk allowed vlan 10,20,99
BranchSwitch(config-if)# exit
```

Replace 99 with any additional VLANs you need to carry.

Spanning Tree Protocol (STP) Configuration

STP prevents loops in a network with redundant links. The Cisco 3560 supports Rapid Spanning Tree Protocol (RSTP) by default. To fine tune it:

Enabling RSTP

```
BranchSwitch(config)# spanning-tree mode rapid-pvst
```

Adjusting Priority for Root Selection

If you want this switch to become the root bridge for a particular VLAN, reduce its priority:

```
BranchSwitch(config)# spanning-tree vlan 10 root primary
```

Higher priority values (default 32768) make the switch less likely to become root.

Port Security and Network Access Control

Basic Port Security

Limit the number of MAC addresses on a port to reduce the risk of MAC flooding:

```
BranchSwitch(config)# interface Ethernet0/2
BranchSwitch(config-if)# switchport port-security
BranchSwitch(config-if)# switchport port-security maximum 2
BranchSwitch(config-if)# switchport port-security violation shutdown
```

```
BranchSwitch(config-if)# exit
```

802.1X Authentication

For environments requiring user authentication, enable 802.1X:

```
BranchSwitch(config)# dot1x system-auth-control
BranchSwitch(config)# interface Ethernet0/2
BranchSwitch(config-if)# switchport mode access
BranchSwitch(config-if)# authentication host-mode single-host
BranchSwitch(config-if)# authentication port-control auto
BranchSwitch(config-if)# exit
```

Ensure you have a RADIUS server configured to validate credentials.

Quality of Service (QoS) Settings

Defining Traffic Classes

Classify traffic using class maps:

```
BranchSwitch(config)# class-map match-any Voice
BranchSwitch(config-cmap)# match access-group 101
BranchSwitch(config-cmap)# exit
```

Creating Policy Maps

Assign bandwidth limits or priorities:

```
BranchSwitch(config)# policy-map QoS-Policy
BranchSwitch(config-pmap)# class Voice
BranchSwitch(config-pmap)# priority 200
BranchSwitch(config-pmap)# exit
```

Applying QoS to Interfaces

Attach the policy to an interface:

```
BranchSwitch(config)# interface Ethernet0/2
BranchSwitch(config-if)# service-policy output QoS-Policy
BranchSwitch(config-if)# exit
```

Layer 3 Routing on the 3560

Enabling IP Routing

Activate routing capabilities:

```
BranchSwitch(config)# ip routing
```

Configuring a Static Route

For simple networks, add a static default route:

BranchSwitch(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1

Dynamic Routing with OSPF

For larger environments, set up OSPF:

BranchSwitch(config)# router ospf 1
BranchSwitch(config-router)# network 192.168.10.0 0.0.0.255 area 0
BranchSwitch(config-router)# exit

Security Hardening Practices

- Disable unused ports with shutdown.
- Enable port security and 802.1X where appropriate.
- Use strong passwords and enable secret encryption.
- Restrict VTY access to specific IP ranges.
- Implement SNMP v3 for secure monitoring.

Monitoring and Troubleshooting

Basic Status Commands

Check interface status:

BranchSwitch# show interfaces status

View VLAN membership:

BranchSwitch# show vlan brief

Spanning Tree Information

Verify STP operation:

BranchSwitch# show spanning-tree

Debugging Port Security

Monitor port security events:

BranchSwitch# show log | include Port security

Logging and Syslog

Send logs to a syslog server:

BranchSwitch(config)# logging host 10.10.10.100
BranchSwitch(config)# logging trap debugging

Stack Management and Redundancy

Stack Configuration

To add a switch to a stack, connect the stack cable and assign stack ports:

```
BranchSwitch(config)# stackwise-virtual
BranchSwitch(config)# stackwise-virtual member 2
BranchSwitch(config)# stackwise-virtual priority 100
```

Failover and Redundancy

Use the stack master to provide a single point of management. If the master fails, another switch takes over automatically.

Backup and Restore Configuration

Saving the Configuration

Store the running configuration to non volatile memory:

```
BranchSwitch# copy running-config startup-config
```

Backing Up to TFTP

Transfer the configuration to a TFTP server:

```
BranchSwitch# copy running-config tftp
Address or name of remote host []? 10.10.10.200
Destination filename [running-config]? backup-branch.cfg
```

Tags: #cisco #3560 #configuration #guide