Cisco 3560 Configuration Guide

Introduction to Cisco Catalyst 3560 Configuration

The Cisco Catalyst 3560 Series is a cornerstone of enterprise and campus networking, offering a robust blend of Layer 2 switching and Layer 3 routing capabilities. Known for its reliability, Power over Ethernet (PoE) support, and advanced quality of service (QoS) features, this switch remains a popular choice for network administrators managing access, distribution, and even small core layers. Mastering the **Cisco 3560 Configuration Guide** is essential for anyone looking to deploy a secure, efficient, and scalable network infrastructure. This comprehensive article walks you through fundamental concepts, step-by-step command examples, and best practices to help you configure your Cisco 3560 switch from initial setup to advanced networking features.

Whether you are preparing for a CCNA exam, upgrading a legacy network, or deploying a new branch office, understanding both the graphical and command-line interface (CLI) approaches will empower you to optimize performance and troubleshoot effectively. Let's dive into the practical configuration that transforms a stock Catalyst 3560 into a finely tuned networking powerhouse.

Initial Setup and Basic Configuration

Connecting to the Cisco 3560

Before any configuration can begin, you must establish a connection to the switch. The most common method is through a console cable connected to the console port on the front panel and a serial-to-USB adapter on your computer. Use a terminal emulation program such as PuTTY, Tera Term, or SecureCRT with the following settings:

- Baud rate: 9600
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None

Once connected, you will see the **Switch>** prompt, indicating user EXEC mode. Type **enable** to enter privileged EXEC mode (**Switch#**), and then **configure terminal** to enter global configuration mode (**Switch(config)#**).

Configuring Basic System Parameters

Setting the hostname, passwords, and management IP address are the first steps in any Cisco 3560 configuration guide. Use the following commands as a template:

1. **Configure the hostname:** *hostname Access-Switch-01*
2. **Set enable secret password:** *enable secret YourStrongPassword*
3. **Create a local user:** *username admin secret adminPassword*
4. **Configure the management VLAN interface:** *interface vlan 1* then *ip address 192.168.1.10 255.255.255.0*
5. **Set default gateway:** *ip default-gateway 192.168.1.1*
6. **Enable SSH for remote access:** *ip domain-name example.local*, *crypto key generate rsa modulus 1024*, then *line vty 0 15* with *transport input ssh* and *login local*.

Always save your configuration using **copy running-config startup-config** or **write memory** to avoid losing settings after a reboot.

Configuring VLANs and Trunking

Creating and Managing VLANs

Virtual LANs (VLANs) segment broadcast domains, improving security and network efficiency. On the Cisco 3560, creating VLANs is straightforward. In global configuration mode, type **vlan 10** and optionally name it, such as **name Sales**. Repeat for each required VLAN, for example, VLAN 20 (Marketing) and VLAN 30 (Engineering).

To assign switch ports to a specific VLAN, enter **interface fastEthernet 0/1** or **interface gigabitEthernet 0/1**, then use the command **switchport mode access** and **switchport access vlan 10**. This places the port in the appropriate VLAN instantly.

For ports that connect to other switches or routers, you must configure trunking. Trunk links carry traffic from multiple VLANs using IEEE 802.1Q encapsulation. Configure a trunk interface with:

- **switchport mode trunk**
- **switchport trunk allowed vlan 10,20,30** (or *all* to permit all VLANs)
- **switchport trunk native vlan 99** (best practice to change the native VLAN from default 1)

Proper VLAN and trunk configuration reduces security risks, such as VLAN hopping attacks, and ensures efficient traffic flow across your network.

Configuring Voice VLANs for IP Telephony

The Cisco 3560 is widely deployed in environments with Cisco IP phones. To separate voice and data traffic on the same physical port, configure a voice VLAN. For example, on interface **FastEthernet 0/2**:

- **switchport mode access**
- **switchport access vlan 50** (data VLAN)
- **switchport voice vlan 60** (voice VLAN)
- **mls qos trust cos** (to trust the Class of Service marking from the phone)

This configuration ensures quality of service for voice traffic while keeping data isolated, a hallmark of a well-designed network.

Securing the Switch and Ports

Port Security

Securing access ports prevents unauthorized devices from connecting to the network. Port security limits the number of MAC addresses allowed on a port. For example, to allow only one MAC address on interface **GigabitEthernet 0/1**:

- **switchport port-security**
- **switchport port-security maximum 1**
- **switchport port-security violation shutdown**
- **switchport port-security mac-address sticky**

The **sticky** option dynamically learns the MAC address and adds it to the running configuration. If a violation occurs, the port will be shut down and must be manually re-enabled using **no shutdown**. This is a simple yet powerful layer of defense.

Storm Control and BPDU Guard

Broadcast storms can cripple a network. Enable broadcast storm control on access ports with **storm-control broadcast level 10** to limit broadcast traffic to 10% of bandwidth. Additionally, enable **BPDU guard** on ports where you do not expect to receive spanning-tree bridge protocol data units (BPDUs). Use **spanning-tree bpduguard enable** on the interface. This feature automatically errdisables the port if a BPDU is received, preventing potential loops caused by unauthorized switches.

Spanning Tree Protocol (STP) Configuration

Rapid Spanning Tree (RSTP) and PVST+

The Cisco 3560 supports Per-VLAN Spanning Tree Plus (PVST+), which runs a separate STP instance for each VLAN. To improve convergence time, enable Rapid Spanning Tree Protocol (RSTP) by using **spanning-tree mode rapid-pvst** in global configuration mode. This setting allows the network to recover from link failures in just a few seconds, rather than the 30–50 seconds typical of classic STP.

Root Bridge Selection

Manually designate the root bridge for each VLAN to ensure deterministic network topology. For VLAN 10, use the command **spanning-tree vlan 10 root primary** on the desired core switch. This sets the bridge priority to 24576. For a backup root, use **spanning-tree vlan 10 root secondary** (priority 28672). On the 3560, you can also adjust **spanning-tree vlan 10 priority 4096** for finer control.

Always verify STP status with **show spanning-tree vlan 10** to confirm the root bridge and port roles. Proper STP configuration prevents loops and ensures high availability.

Layer 3 Routing and Inter-VLAN Communication

Configuring SVIs (Switch Virtual Interfaces)

One of the powerful features of the Catalyst 3560 is its ability to route between VLANs using Layer 3 SVIs. This eliminates the need for an external router. Enable IP routing with **ip routing** in global configuration mode. Then create an SVI for each VLAN:

- **interface vlan 10**
- **ip address 192.168.10.1 255.255.255.0**
- **no shutdown**

Repeat for VLAN 20 and 30 with appropriate IP addresses. Now, traffic between VLANs will be routed by the switch itself. Verify connectivity with **ping** from one VLAN host to another.

Static Routing and Dynamic Routing (OSPF)

To connect the 3560 to other networks or the internet, configure either static routes or a dynamic routing protocol. For a small network, static routes are simple: **ip route 0.0.0.0 0.0.0.0 192.168.1.1** sets a default route. For larger environments, enable OSPF: **router ospf 1**, then **network 192.168.10.0 0.0.0.255 area 0**. The 3560 can participate fully in OSPF, EIGRP, and RIP, making it a versatile Layer 3 switch for diverse network designs.

Remember that the 3560 supports up to 16K MAC addresses and thousands of routes, but always monitor CPU and memory utilization to avoid overloading the switch.

Quality of Service (QoS) for Traffic Prioritization

Classifying and Marking Traffic

QoS ensures that time-sensitive traffic like voice and video gets preferential treatment. On the Cisco 3560, you can classify traffic based on access control lists (ACLs) or by trusting existing markings. For example, to trust the CoS value from a Cisco IP phone:

- **mls qos trust cos** on the interface.

To classify traffic based on a specific protocol, create a class map:

- **class-map match-all VOICE**
- **match ip dscp ef** (Expedited Forwarding for voice)

Then create a policy map to apply the desired action, such as bandwidth reservation or priority queuing.

Applying a Service Policy

Attach the policy map to an interface with **service-policy input VOICE-POLICY** or **service-policy output VOICE-POLICY**. For outbound policies, configure the egress queue settings with **wrr-queue** and bandwidth percentages to control traffic shaping. QoS on the 3560 is sophisticated but well-documented; careful planning ensures critical traffic always flows smoothly.

Monitoring and Troubleshooting

Essential Show Commands

A Cisco 3560 configuration guide is incomplete without diagnostic tools. Use these commands regularly:

- **show running-config –** view current configuration.
- **show interface status –** see port status, VLAN, and duplex.
- **show vlan brief –** list all VLANs and their ports.
- **show ip interface**