



# CHAPTER 28

## Working with Configuration Files

---

This chapter describes how to work with the switch configuration files on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

---

**Note**

The flash device names (such as **slot0:**) differ depending on the type of supervisor engine. See the “[Understanding How the Flash File System Works](#)” section on page 26-1 for details.

---

This chapter consists of these sections:

- [Working with the Configuration Files on the Switch](#), page 28-1
- [Working with the Configuration Files on the MSFC](#), page 28-12

## Working with the Configuration Files on the Switch

These sections describe how to work with the configuration files on the switch:

- [Creating and Using Configuration File Guidelines](#), page 28-2
- [Creating a Configuration File](#), page 28-2
- [Downloading the Configuration Files to the Switch Using TFTP](#), page 28-3
- [Uploading the Configuration Files to a TFTP Server](#), page 28-5
- [Copying the Configuration Files Using SCP or rep](#), page 28-6
- [Downloading the Configuration Files from an rcp or SCP Server](#), page 28-7
- [Uploading Configuration Files to an rcp or SCP Server](#), page 28-8
- [Clearing the Configuration](#), page 28-9
- [Comparing the Configuration Files](#), page 28-10
- [Creating the Configuration Checkpoint Files for Configuration Rollback](#), page 28-11

**Note**

For more information on working with the configuration files on the flash file system, see [Chapter 26](#), “[Working With the Flash File System](#).”

---

## Creating and Using Configuration File Guidelines

- configure the switch. If you configure the switch from a Telnet session, the IP addresses are not changed, and the ports and the modules are not disabled.
- If no passwords have been set on the switch, you must set them on each switch by entering the **set password** and **set enablepass** commands. Enter a blank line after the **set password** and **set enablepass** commands. The passwords are saved in the configuration file as clear text.  
If the passwords already exist, you cannot enter the **set password** and **set enablepass** commands because the password verification will fail. If you enter the passwords in the configuration file, the switch mistakenly attempts to execute the passwords as commands as it executes the file.
- Certain commands must be followed by a blank line in the configuration file. The blank line is necessary; without the blank line, these commands might disconnect your Telnet session. Before disconnecting a session, the switch prompts you for confirmation. The blank line acts as a carriage return, which indicates a negative response to the prompt and retains the Telnet session.

Include a blank line after each occurrence of these commands in a configuration file:

- **set interface sc0** *ip\_addr netmask*
- 
- **set module disable** *mod*
- set port disable** *mod/port*

---

### Step 1

**Step 2** Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.

**Step 3** Extract the portion of the configuration file with the desired commands and save it in a new file. Make sure that the file begins with the word **begin** on a line by itself and ends with the word **end** on a line by itself.

**Step 4** Copy the configuration file to the appropriate TFTP directory on the workstation ( tftplib on a UNIX workstation).

**Step 5** Make sure that the permissions on the file are set to world-read.

---

This example shows an example configuration file. This file could be used to set the Domain Name System (DNS) configuration on multiple switches.

```
begin
!
#dns
set ip dns server 172.16.10.70 primary
set ip dns server 172.16.10.140
set ip dns enable
set ip dns domain corp.com
end
```

## Downloading the Configuration Files to the Switch Using TFTP

You can configure the switch using the configuration files that you create or download from another switch. In addition, you can store the configuration files on the flash devices on the hardware that supports the flash file system, and you can configure the switch using a configuration that is stored on a flash device.

These sections describe how to configure the switch using the configuration files that are downloaded from a TFTP server or that are stored on a flash device:

- [Preparing to Download a Configuration File Using TFTP, page 28-3](#)
- [Configuring the Switch Using a File on a TFTP Server, page 28-4](#)
- [Configuring the Switch Using a File on a Flash Device, page 28-4](#)

## Preparing to Download a Configuration File Using TFTP

Before you begin downloading a configuration file using TFTP, do the following:

- Ensure that the workstation acting as the TFTP server is configured properly. On a Sun workstation, make sure that the `/etc/inetd.conf` file contains this line:

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

Make sure that the `/etc/services` file contains this line:

```
tftp 69/udp
```

**Note**

You must restart the `inetd` daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the `inetd` process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). Refer to the documentation for your workstation for more information on using the TFTP daemon.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route the traffic between the subnets. Check the connectivity to the TFTP server using the **ping** command.
- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server ( `tftpboot` on a UNIX workstation).
- Ensure that the permissions on the file are set correctly. The permissions on the file should be set to world-read.

## Configuring the Switch Using a File on a TFTP Server

---

**Step 1****Step 2** Log into the switch through the console port or a Telnet session.**Step 3** Configure the switch using the configuration file that is downloaded from the TFTP server with the **copy tftp config** command. Specify the IP address or host name of the TFTP server and the name of the file to download.

The configuration file downloads and the commands are executed as the file is parsed line by line.

---

This example shows how to configure the switch using a configuration file that is downloaded from a TFTP server:

```
Console> (enable) copy tftp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using tftp:dns-config.cfg (y/n) [n]? y
/
Finished network download. (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

---

*file-id*

---

```
copy slot0:dns-config.cfg config
```

```
y
```

## Uploading the Configuration Files to a TFTP Server

- 
- 

## Preparing to Upload a Configuration File to a TFTP Server

- 



Note

- 

- 

touch

-

## Uploading a Configuration File to a TFTP Server

Step 1

Step 2

`copy config tftp`

```

copy config tftp
                               172.20.52.3
                               cat6000_config.cfg

Upload configuration to tftp:cat6000_config.cfg, (y/n) [n]?
.....
.....
.....

.....
.....
..
/
Configuration has been copied successfully.
Console> (enable)

```

## Copying the Configuration Files Using SCP or rcp

- 
- 

### rcp Overview

## SCP Overview

## Downloading the Configuration Files from an rcp or SCP Server

- 
- 

## Preparing to Download a Configuration File Using rcp or SCP

- 
- 
- 
- 

username will be stored in NVRAM. If you are accessing the switch through a Telnet session with a valid username, this username will be used and there is no need to set the rcp username.

## Configuring the Switch Using a File on an rcp or SCP Server

To configure a Catalyst 6500 series switch using a configuration file that is downloaded from an rcp or SCP server, perform these steps:

- 
- Step 1** Copy the configuration file to the appropriate directory on the workstation.
  - Step 2** Log into the switch through the console port or a Telnet session. If you are using SCP, log in using an SSH session.
  - Step 3** Configure the switch using the configuration file that is downloaded from the server by entering the **rcp | scp config** command. Specify the IP address or host name of the server and the name of the file to download.

The configuration file downloads and the commands are executed as the file is parsed line by line.

---

This example shows how to configure a Catalyst 6500 series switch using a configuration file that is downloaded from a server:

```
Console> (enable) copy rcp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using rcp:dns-config.cfg (y/n) [n]? y
/
Finished network download. (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

**ping**

---

**copy config rcp | scp**

---

```

Console> (enable) copy config rcp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat6000_config.cfg

Upload configuration to rcp:cat6000_config.cfg, (y/n) [n]? y
.....
.....
.....

.....
.....
..
/
Configuration has been copied successfully.
Console> (enable)

```

```

Console> (enable) copy scp flash scp
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup720cvk9.8-3-1.bin
Username for scp[bob]?
Password for User bob[:
CCC/
File has been copied successfully.

```

Task	Command

```

Console> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the next system startup.
Do you want to continue (y/n) [n]? y
.....
.....

System configuration cleared.
Console> (enable)

```

Task	Command

**Note**

```

Console> (enable) clear config 2
This command will clear module 2 configuration.
Do you want to continue (y/n) [n]? y
.....
Module 2 configuration cleared.
Console> (enable)

```

Task	Command
	{   }

## Comparing the Configuration Files

Task	Command
Compare the differences between the configuration files.	<code>file   ignorecase {   context val  </code>

```

Console> (enable) show config differences 1.cfg 2.cfg
--- bootflash:1.cfg
+++ bootflash:2.cfg
@@ -8,1 +8,1 @@
-#version 8.2(0.11-Eng)DEL
+#VERSION 8.2(0.11-eNG)del
@@ -11,1 +11,1 @@
-set config mode text auto-save interval 1
+SET CONFIG MODE TEXT AUTO-SAVE INTERVAL 1
Console> (enable)

```

```

Console> (enable) show config differences ignorecase 1.cfg 2.cfg
Files bootflash:1.cfg and bootflash:2.cfg are identical
Console> (enable)

```

## Creating the Configuration Checkpoint Files for Configuration Rollback

files quickly and with the least possible disturbance to switch functionality.

Follow these guidelines when creating the configuration checkpoint files:

- A configuration checkpoint file is identified by a name that you specify when you create the file. The configuration checkpoint filename can be no more than 15 characters. If you do not specify a name, the system generates one. The system-generated name is in the format CKPi\_MMDDYYHHMM, where “i” represents a checkpoint number.
- The checkpoint file is stored either on the bootflash or on slotX/diskX. If you do not specify a device, the file is stored on the current default device.
- The configuration checkpoint file is stored as a text file that can be read and edited. We strongly advise that you do not edit the file.
- When a checkpoint filename is cleared from the system, the associated configuration checkpoint file is deleted. You should squeeze the device to reclaim space.
- You can create a maximum of five configuration checkpoint files on a system. You can roll back to any of the saved configuration checkpoint files in any order. Because these files are generated using a complete configuration, they are independent of each other.
- The checkpoint configuration is stored in NVRAM. The configuration is not cleared when you enter the **clear config all** command.
- This feature is supported on the systems with redundant supervisor engines. The checkpoint configuration and its associated files are synchronized to the standby supervisor engine.

To create a configuration checkpoint file, perform this task in privileged mode:

Create a configuration checkpoint file.	<b>set config checkpoint</b> [ <i>name name</i> ] [ <i>device device</i> ]
Verify the configuration checkpoint filename.	<b>show config checkpoints</b>

This example shows how to create a configuration checkpoint file and verify that it has been created:

```
Configuration checkpoint CKP0_0722040905 creation successful.
Console> (enable)
Checkpoint          File id              Date
=====
CKP0_0722040905    bootflash:CKP0_07220409058.4(0.79)COC  Thu Jul 22 2000, 09:05:31
Console> (enable)
```

To roll the current configuration file back to a previously created configuration checkpoint file, perform this task in privileged mode:

Task	Command
Roll the current configuration file back to a configuration checkpoint file.	<b>set config rollback</b>

To clear all the configuration checkpoint files or a particular configuration checkpoint file, perform this task in privileged mode:

Task	Command
Clear all configuration checkpoint files or a particular configuration checkpoint file.	<b>clear config checkpoint {all          }</b>
Verify the configuration checkpoint filenames.	<b>show config checkpoints</b>

This example shows how to clear all configuration checkpoint files and to verify that they have been cleared:

```

Console> (enable)
All configuration checkpoints cleared.
Console> (enable)
No Checkpoints defined.
Console> (enable)
    
```

## Working with the Configuration Files on the MSFC

These sections describe how to work with the configuration files on the Multilayer Switch Feature Card (MSFC):

- [Uploading the Configuration File to a TFTP Server, page 28-13](#)
- [Uploading the Configuration File to the Supervisor Engine Flash PC Card, page 28-14](#)
- [Downloading the Configuration File from a Remote Host, page 28-14](#)
- [Downloading the Configuration File from the Supervisor Engine Flash PC Card, page 28-16](#)

The configuration information resides in two places when the MSFC is operating: the default (permanent) configuration in NVRAM and the running (temporary) memory in RAM. The default configuration always remains available; NVRAM retains the information even when the power is shut down. The current information is lost if the system power is shut down. The current configuration contains all the nondefault configuration information that you added by entering the **configure** command or the **setup** command facility, or by editing the configuration file.

The **copy running-config startup-config** command adds the current configuration to the default configuration in NVRAM, so that it is saved if power is shut down. Whenever you make changes to the system configuration, enter the **copy running-config startup-config** command to save the new configuration.

If you replace the MSFC, you need to replace the entire configuration. If you upload (copy) the configuration file to a remote server before removing the MSFC, you can retrieve it later and write it into NVRAM on the new MSFC. If you do not upload the configuration file, you need to enter the **configure** command to reenter the configuration information after you install the new MSFC.

Saving and retrieving the configuration file is not necessary if you are temporarily removing an MSFC that you are going to reinstall; the lithium batteries retain the configuration in memory. This procedure requires the privileged-level access to the EXEC command interpreter, which usually requires a password.

## Uploading the Configuration File to a TFTP Server

Before you upload the running configuration to the TFTP file server, ensure the following:

- You have a connection to the MSFC either with a console terminal or remotely through a Telnet session.
- The MSFC is connected to a network supporting a file server (remote host).
- The remote host supports the TFTP application.
- You have the IP address or name of the remote host available.

To store information on a remote host, enter the privileged **write network** EXEC command. This command prompts you for the destination host address and a filename and then displays the instructions for confirmation. When you confirm the instructions, the MSFC sends a copy of the currently running configuration to the remote host. The system default is to store the configuration in a file called by the name of the MSFC with *-config* appended. You can either accept the default filename by pressing **Return** at the prompt, or enter a different name before pressing **Return**.

To upload the currently running configuration to a remote host, perform these steps:

- 
- Step 1** Check if the system prompt displays a pound sign (#) to indicate the privileged level of the EXEC command interpreter.
- Step 2** Enter the **ping** command to check the connection between the MSFC and the remote host.
- Step 3** Enter the **write term** command to display the currently running configuration on the terminal and ensure that the configuration information is complete and correct. If it is not correct, enter the **configure** command to add or modify the existing configuration.
- Step 4** Enter the **write net** command. The EXEC command interpreter prompts you for the name or IP address of the remote host that is to receive the configuration file. (The prompt might include the name or address of a default file server.)

```
Router#
Remote host []?
```

- Step 5** Enter the name or IP address of the remote host. In this example, the name of the remote server is *servername*:

```
Router#
Remote host []? servername
Translating "servername"...domain server (1.1.1.1) [OK]
```

- Step 6** Note that the EXEC command interpreter prompts you to specify a name for the file that is to hold the configuration. By default, the system appends *-config* to the MSFC name to create the new filename. Press **Return** to accept the default filename, or enter a different name for the file before pressing **Return**. This example shows that the default is accepted:

```
Name of configuration file to write [Router-config]?
Write file Router-config on host 1.1.1.1? [confirm]
Writing Router-config .....
```

- Step 7** Note that before the MSFC executes the copy process, it displays the instructions that you entered for confirmation. If the instructions are not correct, enter **n** (no) and press **Return** to abort the process. To accept the instructions, press **Return** or **y** (yes) and then press **Return**, and the system begins the copy process. This example shows that the default is accepted:

```
Write file Router-config on host 1.1.1.1? [confirm]
Writing Router-config: !!!! [ok]
```

While the MSFC copies the configuration to the remote host, it displays a series of exclamation points (!!!) or periods (...). The !!! and [ok] indicate that the operation is successful. A display of ... [timed out] or [failed] indicates a failure, which would probably be due to a network fault or the lack of a writable, readable file on the remote file server.

- Step 8** Note that if the display indicates that the process was successful (with the series of !!! and [ok]), the upload process is complete. The configuration is safely stored in the temporary file on the remote file server.

If the display indicates that the process failed (with the series of ... as shown in the following example):

```
Writing Router-config .....
```

your configuration was not saved. Repeat the preceding steps, or select a different remote file server and repeat the preceding steps.

If you are unable to copy the configuration to a remote host successfully, contact your network administrator.

## Uploading the Configuration File to the Supervisor Engine Flash PC Card

To upload the configuration file to the supervisor engine Flash PC card, perform this task:

	Task	Command
<b>Step 1</b>	At the EXEC prompt, enter enable mode.	Router> <b>enable</b>
<b>Step 2</b>	Copy the startup configuration file to slot 0.	Router# <b>copy startup-config sup-slot0:</b>
<b>Step 3</b>	Copy the running configuration file to slot 0.	Router# <b>copy running-config sup-slot0:</b>

## Downloading the Configuration File from a Remote Host

After you install the new MSFC, you can retrieve the saved configuration and copy it to NVRAM. Enter configuration mode and specify that you want to configure the MSFC from the network. The system prompts you for a host name and address, the name of the configuration file that is stored on the host, and confirmation to reboot using the remote file.

To download the currently running configuration from a remote host, perform these steps:

- Step 1** Check if the system prompt displays a pound sign (#) to indicate the privileged level of the EXEC command interpreter.



**Note** Until you retrieve the previous configuration, the MSFC runs from the default configuration in NVRAM. Any passwords that were configured on the previous system are not valid until you retrieve the configuration.

- Step 2** Enter the **ping** command to verify the connection between the router and the remote host.

- Step 3** At the system prompt, enter the **configure network** command and press **Return** to enter configuration mode. Specify that you want to configure the system from a network device (instead of from the console terminal, which is the default).

```
Router# configure network
```

- Step 4** Note that the system prompts you to select a host or network configuration file. The default is host; press **Return** to accept the default.

```
Host or network configuration file [host]?
```

- Step 5** Note that the system prompts you for the IP address of the host. Enter the IP address or name of the remote host (the remote file server to which you uploaded the configuration file).

```
IP address of remote host [255.255.255.255]? 1.1.1.1
```

- Step 6** Note that the system prompts you for the configuration filename. When uploading the file, the default is to use the name of the MSFC with the suffix *(router-confg* in the following example). If you specified a different filename when you uploaded the configuration, enter the filename; otherwise, press **Return** to accept the default.

```
Name of configuration file [router-confg]?
```

- Step 7** Note that before the system reboots with the new configuration, it displays the instructions that you entered for confirmation. If the instructions are not correct, enter **n** (no), and then press **Return** to cancel the process. To accept the instructions, press **Return**, or **y**, and then press **Return**.

```
Configure using router-confg from 1.1.1.1? [confirm]
Booting router-confg from 1.1.1.1: !! [OK - 874/16000 bytes]
```

While the MSFC retrieves and boots from the configuration on the remote host, the console display indicates whether or not the operation was successful. A series of !!!! and [OK] (as shown in the preceding example) indicate that the operation was successful. A series of . . . and [timed out] or [failed] indicate a failure (which would probably be due to a network fault or an incorrect server name, address, or filename). This example shows a failed attempt to boot from a remote server:

```
Booting Router-confg . . . . [timed out]
```

- Step 8** Proceed to the next step if the display indicates that the process was successful.

If the display indicates that the process failed, verify the name or address of the remote server and the filename, and repeat the preceding steps. If you are unable to retrieve the configuration, contact your network administrator.

- Step 9** Enter the **write term** command to display the currently running configuration on the terminal. Review the display and ensure that the configuration information is complete and correct. If it is not, verify the filename and repeat the preceding steps to retrieve the correct file, or enter the **configure** command to add or modify the existing configuration. (See the appropriate software documentation for the configuration options that are available for the system, the individual interfaces, and specific configuration instructions.)
- Step 10** When you verify that the currently running configuration is correct, enter the **copy running-config startup-config** command to save the retrieved configuration in NVRAM. Otherwise, you will lose the new configuration if you restart the system.

## Downloading the Configuration File from the Supervisor Engine Flash PC Card

To download the configuration file from the supervisor engine Flash PC card, perform this task:

	Task	Command
<b>Step 1</b>	At the EXEC prompt, enter enable mode.	Router> <b>enable</b>
<b>Step 2</b>	Copy the stored running configuration file to the MSFC running configuration.	Router# <b>copy sup-slot0: <i>file_name</i> running-config</b>
<b>Step 3</b>	Copy the stored startup configuration file to the MSFC running configuration.	Router# <b>copy sup-slot0: <i>file_name</i> startup-config</b>

## Working with Profile Files

A profile file allows you to have a customized configuration as the default configuration on the switch. The profile file allows you to load a custom default configuration that enables or disables certain features at bootup or when a new module is installed. With the profile files, you can eliminate the features or processes that may pose security risks (for example, disabling CDP or turning off auto-trunking on a port) to your switch.

A profile file that has most of the security risks disabled is also known as a “lockdown” profile. A lockdown profile changes the functionality of the switch from enabling access to preventing access by default. When a lockdown profile is applied, you must manually enable the features that were disabled by the profile file.

## Building Profile Files

The profile file format is similar to the format of a configuration file. You can either create a new profile file or edit a system-generated configuration file.



### Caution

We recommend that you do not create new profile files unless you are familiar with configuration files because missing or misplaced elements will cause the configuration to fail.

If you choose to create the profile files by editing a system-generated configuration file, most of the required notations will already be in the file. The keywords that are currently supported are ALL\_MODULES, ALL\_PORTS, ALL\_MODULE\_PORTS, and ALL\_VLANS. Do not create a profile file using the output that results from entering the **copy config all** command as a template because the output includes default configuration information, which increases the size and processing time of the file.

To designate the system profile file that you want to use, perform this task in privileged mode:

	Task	Command
Step 1	Designate the device and name of the profile filename that you want to use.	<b>set system profile</b> <i>device:filename</i>
Step 2	Enable or disable the system profile files on the specified modules.	<b>set system profile {enable   disable}</b> <i>mod_list</i>

This example shows how to designate the device name and the profile filename:

```
Console> (enable)
System is set to be configured with profile file bootflash:test.cfg.
Console> (enable)
```

This example shows how to disable the system profile loading on a specified module:

```
Console> (enable)
System profile loading is disabled for module 2.
Console> (enable)
```

This example shows a sample lockdown profile file. You can use an exact copy of this file if you want to use what would be considered a typical lockdown profile file as your default configuration. You can also change the file and use the altered version of the file if the parameters of this lockdown profile file does not meet your needs.

```
begin
!
# ***** DEFAULT PROFILE *****
!
#####
# Lockdown Profile version 1.0.3 #
#####
!
# set system prompt (edit as needed)
set prompt locked_down>
!
# system attributes to be customized (edit as needed)
set system name locked_down
set system contact locked_down
set system location locked_down
!
# set a strong banner (edit as needed)
set banner motd ^
Access to this device or the attached networks is prohibited
without express permission from the network administrator.

Violators will be prosecuted to the fullest extent of both civil
and criminal law.
```

```

^
!
!
#
# vtp mode off, enable password and dummy domain (edit as needed)
set vtp domain locked_down
set vtp mode off
set vtp passwd locked_down
!
# default VLAN is "Quarantine" (edit as needed)
set vlan 999 name Quarantine
!
# Management VLAN is "Management" (edit as needed)
set vlan 1000 name Management
# Alternate management vlan is "OtherMgmt" (edit as needed)
set vlan 1001 name OtherMgmt
!
# sc0 and sc1 off (edit as needed)
set interface sc0 down
set interface sc0 1000
set interface sc1 down
set interface sc1 1001
!
# default port status is disabled
set port disable ALL_PORTS
!
# default cdp status is disabled
set cdp disable ALL_PORTS
!
# default STP status is with BPDU guard enabled
set spantree portfast bpdu-guard ALL_PORTS enable
!
# default PAGP/LACP status is disabled
set port channel ALL_PORTS mode off
!
# Default DTP status is disabled, no allowed vlans and dot1q-all-tagged mode on.
# Warning: A max of 128 trunks can have non-default configuration in CatOS 8.4
# Warning: Edit port list as needed.
set trunk ALL_PORTS off none
set dot1q-all-tagged enable
!
# default is CPU rate limiters enabled
set rate-limit l2pdu enable
!
# default SSH version is 2
set ssh mode v2
!
# default VLAN is "Quarantine" (edit as needed)
set vlan 999 ALL_PORTS
!
# Enable image checksum verification by default
set image-verification enable
!
# Set a more aggressive default logout timeout
set logout 10
#
#
# Anti-spoofing ACL
#
!
! Deny any packets from the RFC 1918, IANA reserved, ranges,
! multicast as a source, and loopback netblocks to block
! attacks from commonly spoofed IP addresses.

```

Note that the following ACLs might not be up to date.

```
! Refer to www.iana.org/assignments/ipv4-address-space for a current list.
!
! Bogons
!
set security acl ip Anti-spoofing deny ip 0.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 1.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 2.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 5.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 7.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 10.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 23.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 27.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 31.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 36.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 37.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 39.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 42.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 49.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 50.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 77.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 78.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 79.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 92.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 93.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 94.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 95.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 96.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 97.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 98.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 99.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 100.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 101.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 102.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 103.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 104.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 105.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 106.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 107.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 108.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 109.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 110.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 111.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 112.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 113.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 114.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 115.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 116.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 117.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 118.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 119.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 120.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 121.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 122.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 123.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 127.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 169.254.0.0 0.0.255.255 any log
set security acl ip Anti-spoofing deny ip 172.16.0.0 0.15.255.255 any log
set security acl ip Anti-spoofing deny ip 173.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 174.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 175.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 176.0.0.0 0.255.255.255 any log
```

```
set security acl ip Anti-spoofing deny ip 177.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 178.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 179.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 180.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 181.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 182.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 183.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 184.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 185.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 186.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 187.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 192.0.2.0 0.0.0.255 any log
set security acl ip Anti-spoofing deny ip 192.168.0.0 0.0.255.255 any log
set security acl ip Anti-spoofing deny ip 197.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 223.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 224.0.0.0 31.255.255.255 any log
# Add here a specific list of permits as needed
set security acl ip Anti-spoofing deny any any log
!
# Set protection to VLAN list (edit as needed)
# You can use ALL_VLANS but that will
# take some time to finish.
# Use the "show security acl" cmd to verify when
# the ACL mapping process is completed.
commit security acl all
set security acl map Anti-spoofing ALL_VLANS
!
!
end
```