



## **Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x**

**First Published:** March 05, 2010

**Last Modified:** June 26, 2010

### **Americas Headquarters**

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://cisco.com/go/trademarks>. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1101R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### **Preface** vii

Audience vii

Document Organization vii

Related Documentation viii

Obtaining Documentation and Submitting a Service Request ix

### **Overview** 1

Examples of Fundamental Configurations 1

Examples of Layer 2 Switching Configurations 1

Examples of OTV Configurations 1

Examples of Security Configurations 2

### **Fundamentals Configuration Examples** 3

Defining Command Aliases 3

Using CLI Session Variables 4

Using the System-Defined Timestamp Variable 4

Running a Command Script 5

Accessing Directories on Standby Supervisor Modules 5

Moving Files 6

Copying Files 6

Displaying File Contents 6

Displaying File Checksums 7

Compressing and Uncompressing Files 7

Redirecting show Command Output 7

Finding Files 8

Copying Configuration Files 8

Backing Up Configuration Files 8

Rolling Back to a Previous Configuration 9

### **Layer 2 Switching Configuration Examples** 11

Configuration Example for Layer 2 Switching 11

Configuration Example for VLANs	11
Configuration Examples for Private VLANs	11
MST Example Configuration	12
Configuration Examples for STP Extension	14
<b>Security Configuration Examples</b>	<b>15</b>
Configuration Example for FIPS	16
Configuration Examples for AAA	16
Configuration Example for RADIUS	16
Configuration Examples for TACACS+	16
Configuration Example for SSH	18
Configuration Example for SSH Passwordless File Copy	19
Configuration Examples for PKI	21
Configuring Certificates on a Cisco NX-OS Device	21
Downloading a CA Certificate	23
Requesting an Identity Certificate	28
Revoking a Certificate	35
Generating and Publishing the CRL	37
Downloading the CRL	39
Importing the CRL	42
Configuration Examples for User Accounts and RBAC	44
Configuration Example for 802.1X	45
Configuration Example for NAC	45
Configuration Examples for Cisco TrustSec	45
Enabling Cisco TrustSec	46
Configuring AAA for Cisco TrustSec on a Seed Cisco NX-OS Device	46
Enabling Cisco TrustSec Authentication on an Interface	46
Configuring Cisco TrustSec Authentication in Manual Mode	46
Configuring Cisco TrustSec Role-Based Policy Enforcement for the default VRF	47
Configuring Cisco TrustSec Role-Based Policy Enforcement for a Nondefault VRF	47
Configuring Cisco TrustSec Role-Based Policy Enforcement for a VLAN	47
Configuring IPv4 Address to SGACL SGT Mapping for the Default VRF	47
Configuring IPv4 Address to SGACL SGT Mapping for a Nondefault VRF	47
Configuring IPv4 Address to SGACL SGT Mapping for a VLAN	48
Manually Configuring Cisco TrustSec SGACLs	48
Manually Configuring SXP Peer Connections	49

Configuration Examples for IP ACLs	49
Configuration Example for MAC ACLs	51
Configuration Example for VACLs	51
Configuration Example for Port Security	51
Configuration Examples for DHCP	51
Configuration Examples for DAI	52
Example 1 Two Devices Support DAI	52
Configuring Device A	53
Configuring Device B	54
Example 2 One Device Supports DAI	56
Configuration Example for IP Source Guard	58
Configuration Examples for Password Encryption	58
Configuration Example for Keychain Management	59
Configuration Example for Traffic Storm Control	59
Configuration Examples for Unicast RPF	59
Configuration Examples for CoPP	60
CoPP Configuration Example	60
Changing or Reapplying the Default CoPP Policy Using the Setup Utility	61
Preventing CoPP Overflow by Splitting ICMP Pings and ARP Requests	62
Configuration Examples for Rate Limits	63
<b>OTV Configuration Examples</b>	<b>65</b>
Configuration Examples for OTV	65
Load Balancing Example	66





## Preface

---

This preface describes the audience and organization of the *Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x*. It also provides information on how to obtain related documentation.

- [Audience, page vii](#)
- [Document Organization, page vii](#)
- [Related Documentation, page viii](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

## Audience

This publication is for experienced users who configure and maintain Cisco NX-OS devices.

## Document Organization

This document is organized into the following chapters:

Chapter	Description
"Overview"	Provides configuration examples of commonly used features for the Cisco Nexus 7000 Series devices.
"Fundamentals Configuration Examples"	Provides examples for configuring certain fundamental Cisco NX-OS features.
"Layer 2 Switching Configuration Examples"	Provides examples for configuring Layer 2 switching.
"OTV Configuration Examples"	Provides examples for configuring Overlay Transport Virtualization (OTV).
"Security Configuration Examples"	Provides examples for configuring security features.

# Related Documentation

Cisco NX-OS documentation is available at the following URL:

[http://www.cisco.com/en/US/products/ps9372/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html)

The documentation set for the Cisco NX-OS software includes the following documents:

## Release Notes

*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*

## NX-OS Configuration Guides

*Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x*

*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*

*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*

*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*

*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide*

*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*

*Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*

*Cisco Nexus 7000 Series OTV Quick Start Guide*

*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*

*Configuring Feature Set for FabricPath*

*Configuring the Cisco Nexus 2000 Series Fabric Extender*

## NX-OS Command References

*Cisco Nexus 7000 Series NX-OS Command Reference Master Index*

*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*

*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*

*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Command Reference*

*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*



*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*  
*Cisco Nexus 7000 Series NX-OS LISP Command Reference*  
*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*  
*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*  
*Cisco Nexus 7000 Series NX-OS OTV Command Reference*  
*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*  
*Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*  
*Cisco Nexus 7000 Series NX-OS Security Command Reference*  
*Cisco Nexus 7000 Series NX-OS System Management Command Reference*  
*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*  
*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*  
*Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*

**Other Software Document**

*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*  
[Cisco Nexus 7000 Series NX-OS MIB Quick Reference](#)  
*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x*  
[Cisco Nexus 7000 Series NX-OS Troubleshooting Guide](#)  
*Cisco NX-OS Licensing Guide*  
[Cisco NX-OS System Messages Reference](#)  
*Cisco NX-OS XML Interface User Guide*

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





# CHAPTER 1

## Overview

---

The *Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x* provides some examples of commonly used features for the Cisco Nexus 7000 Series devices.

For detailed information on each feature, including guidelines and limitations, system defaults, and configuration limits, see the corresponding configuration guide.

- [Examples of Fundamental Configurations, page 1](#)
- [Examples of Layer 2 Switching Configurations, page 1](#)
- [Examples of OTV Configurations, page 1](#)
- [Examples of Security Configurations, page 2](#)

## Examples of Fundamental Configurations

This document contains examples of how to configure fundamental features for the Cisco Nexus 7000 Series devices. It includes examples for using the command-line interface (CLI), using the file system, and working with configuration files.

## Examples of Layer 2 Switching Configurations

This document contains examples of how to configure basic Layer 2 switching features for the Cisco Nexus 7000 Series devices. It includes examples for configuring VLANs, private VLANs, Multiple Spanning Tree (MST), and Cisco-proprietary extensions for the Spanning Tree Protocol (STP).

## Examples of OTV Configurations

This document contains examples of how to configure the Overlay Transport Virtualization (OTV) feature for the Cisco Nexus 7000 Series devices. It includes examples for the basic OTV setup and for using OTV for load balancing.

# Examples of Security Configurations

This document contains examples of how to configure security features for the Cisco Nexus 7000 Series devices. It includes examples for configuring access control lists (ACLs), DHCP snooping, and control plane policing (COPP) as well as many other security features.



## CHAPTER 2

# Fundamentals Configuration Examples

---

This chapter provides examples for configuring certain fundamental Cisco NX-OS features.

- [Defining Command Aliases, page 3](#)
- [Using CLI Session Variables, page 4](#)
- [Using the System-Defined Timestamp Variable, page 4](#)
- [Running a Command Script, page 5](#)
- [Accessing Directories on Standby Supervisor Modules, page 5](#)
- [Moving Files, page 6](#)
- [Copying Files, page 6](#)
- [Displaying File Contents, page 6](#)
- [Displaying File Checksums, page 7](#)
- [Compressing and Uncompressing Files, page 7](#)
- [Redirecting show Command Output, page 7](#)
- [Finding Files, page 8](#)
- [Copying Configuration Files, page 8](#)
- [Backing Up Configuration Files, page 8](#)
- [Rolling Back to a Previous Configuration, page 9](#)

## Defining Command Aliases

This example shows how to define command aliases:

```
cli alias name ethint interface ethernet
cli alias name shintbr show interface brief
cli alias name shintupbr shintbr | include up | include ethernet
```

This example shows how to use a command alias:

```
switch# configure terminal
switch(config)# ethint 2/3
switch(config-if)#
```

## Using CLI Session Variables

You can reference a variable using the syntax `$(variable-name)`.

This example shows how to reference a user-defined CLI session variable:

```
switch# show interface $(testinterface)
Ethernet2/1 is down (Administratively down)
  Hardware is 10/100/1000 Ethernet, address is 0000.0000.0000 (bia 0019.076c.4dac)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters never
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun 0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause 0 reset
```

## Using the System-Defined Timestamp Variable

This example uses `$(TIMESTAMP)` when redirecting `show` command output to a file:

```
switch# show running-config > rcfg.$(TIMESTAMP)
Preparing to copy...done
switch# dir
  12667      May 01 12:27:59 2008  rcfg.2008-05-01-12.27.59

Usage for bootflash://sup-local
8192 bytes used
20963328 bytes free
20971520 bytes total
```

## Running a Command Script

This example displays the CLI commands specified in the script file:

```
switch# show file testfile
configure terminal
interface ethernet 2/1
no shutdown
end
show interface ethernet 2/1
```

This example displays the **run-script** command execution output:

```
switch# run-script testfile
`configure terminal`
`interface ethernet 2/1`
`no shutdown`
`end`
`show interface ethernet 2/1`
Ethernet2/1 is down (Link not connected)
  Hardware is 10/100/1000 Ethernet, address is 0019.076c.4dac (bia 0019.076c.4dac)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters 1d26.2uh
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun 0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause 0 reset
```

## Accessing Directories on Standby Supervisor Modules

This example shows how to list the files on the standby supervisor module:

```
switch# dir bootflash://sup-remote
12198912   Aug 27 16:29:18 2003  m9500-sflek9-kickstart-mzg.1.3.0.39a.bin
 1864931   Apr 29 12:41:59 2003  dplug2
   12288   Apr 18 20:23:11 2003  lost+found/
12097024   Nov 21 16:34:18 2003  m9500-sflek9-kickstart-mz.1.3.1.1.bin
41574014   Nov 21 16:34:47 2003  m9500-sflek9-mz.1.3.1.1.bin
```

```
Usage for bootflash://sup-remote
```

```
67747169 bytes used
116812447 bytes free
184559616 bytes total
```

This example shows how to delete a file on the standby supervisor module:

```
switch# delete bootflash://sup-remote/aOldConfig.txt
```

## Moving Files

This example shows how to move a file on an external flash device:

```
switch# move slot0:samplefile slot0:mystorage/samplefile
```

This example shows how to move a file in the default file system:

```
switch# move samplefile mystorage/samplefile
```

## Copying Files

This example shows how to copy the file called samplefile from the root directory of the slot0: file system to the mystorage directory:

```
switch# copy slot0:samplefile slot0:mystorage/samplefile
```

This example shows how to copy a file from the current directory level:

```
switch# copy samplefile mystorage/samplefile
```

This example shows how to copy a file from the active supervisor module bootflash to the standby supervisor module bootflash:

```
switch# copy bootflash:system_image bootflash://sup-2/system_image
```

This example shows how to overwrite the contents of an existing configuration in NVRAM:

```
switch# copy nvram:snapshot-config nvram:startup-config
```

```
Warning: this command is going to overwrite your current startup-config:
Do you wish to continue? {y/n} [y] y
```

You can also use the **copy** command to upload and download files from the slot0: or bootflash: file system to or from a FTP, TFTP, SFTP, or SCP server.

## Displaying File Contents

This example displays the contents of a file on an external flash device:

```
switch# show file slot0:test
configure terminal
interface ethernet 1/1
no shutdown
end
show interface ethernet 1/1
```



This example displays the contents of a file residing in the current directory:

```
switch# show file myfile
```

## Displaying File Checksums

This example shows how to display the checksum of a file:

```
switch# show file bootflash:trunks2.cfg cksum
583547619
```

This example shows how to display the MD5 checksum of a file:

```
switch# show file bootflash:trunks2.cfg md5sum
3b94707198aabefcf46459de10c9281c
```

## Compressing and Uncompressing Files

This example shows how to compress a file:

```
switch# dir
 1525859      Jul 04 00:51:03 2003 Samplefile
...
switch# gzip volatile:Samplefile
switch# dir
 266069      Jul 04 00:51:03 2003 Samplefile.gz
...
```

This example shows how to uncompress a compressed file:

```
switch# dir
 266069      Jul 04 00:51:03 2003 Samplefile.gz
...
switch# gunzip samplefile
switch# dir
 1525859      Jul 04 00:51:03 2003 Samplefile
...
```

## Redirecting show Command Output

This example shows how to direct the output to a file on the bootflash: file system:

```
switch# show interface > bootflash:switch1-intf.cfg
```

This example shows how to direct the output to a file on external flash memory:

```
switch# show interface > slot0:switch-intf.cfg
```

This example shows how to direct the output to a file on a TFTP server:

```
switch# show interface > tftp://10.10.1.1/home/configs/switch-intf.cfg
Preparing to copy...done
```

This example directs the output of the **show tech-support** command to a file:

```
switch# show tech-support > Samplefile
Building Configuration ...
switch# dir
 1525859      Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
 1527808 bytes used
19443712 bytes free
20971520 bytes total
```

## Finding Files

This example shows how to find a file in the current default directory:

```
switch# find smm_shm.cfg
/usr/bin/find: ../lost+found: Permission denied
./smm_shm.cfg
./newer-fs/isan/etc/routing-sw/smm_shm.cfg
./newer-fs/isan/etc/smm_shm.cfg
```

## Copying Configuration Files

This example shows how to overwrite the contents of an existing configuration in NVRAM:

```
switch# copy nvram:snapshot-config nvram:startup-config
Warning: this command is going to overwrite your current startup-config.
Do you wish to continue? {y/n} [y] y
```

This example shows how to copy a running configuration to the bootflash: file system:

```
switch# copy system:running-config bootflash:my-config
```

## Backing Up Configuration Files

This example shows how to create a snapshot of the startup configuration in a predefined location on the device (binary file):

```
switch# copy startup-config nvram:snapshot-config
```

This example shows how to back up the startup configuration to the bootflash: file system (ASCII file):

```
switch# copy startup-config bootflash:my-config
```

This example shows how to back up the startup configuration to the TFTP server (ASCII file):

```
switch# copy startup-config tftp://172.16.10.100/my-config
```

This example shows how to back up the running configuration to the bootflash: file system (ASCII file):

```
switch# copy running-config bootflash:my-config
```

## Rolling Back to a Previous Configuration

To roll back your configuration to a snapshot copy of a previously saved configuration, you need to perform the following steps:

- 1 Clear the current running image with the **write erase** command.
- 2 Restart the device with the **reload** command.
- 3 Copy the previously saved configuration file to the running configuration with the **copy *configuration\_file* running-configuration** command.
- 4 Copy the running configuration to the start-up configuration with the **copy running-config startup-config** command.





## CHAPTER 3

# Layer 2 Switching Configuration Examples

This chapter provides examples for configuring Layer 2 switching.

- [Configuration Example for Layer 2 Switching, page 11](#)
- [Configuration Example for VLANs, page 11](#)
- [Configuration Examples for Private VLANs, page 11](#)
- [MST Example Configuration, page 12](#)
- [Configuration Examples for STP Extension, page 14](#)

## Configuration Example for Layer 2 Switching

The following example shows how to add a static MAC address and how to modify the default global aging time for MAC addresses:

```
switch# configure terminal
switch(config)# mac address-table static 0000.0000.1234 vlan 10 interface ethernet 2/15
switch(config)# mac address-table aging-time 120
```

## Configuration Example for VLANs

The following example shows how to create and name a VLAN as well as how to make the state active and administratively up:

```
switch# configure terminal
switch(config)# vlan 10
switch(config-vlan)# name test
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
switch(config)#
```

## Configuration Examples for Private VLANs

The following example shows how to create the three types of private VLANs, how to associate the secondary VLANs to the primary VLAN, how to create a private VLAN host and promiscuous port and assign them to

the correct VLAN, and how to create a VLAN interface, or SVI, to allow the primary VLAN to communicate with the rest of the network:

```
switch# configure terminal
switch(config)# vlan 2
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)# vlan 3
switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# vlan 4
switch(config-vlan)# private-vlan isolated
switch(config-vlan)# exit

switch(config)# vlan 2
switch(config-vlan)# private-vlan association 3,4
switch(config-vlan)# exit

switch(config)# interface ethernet 1/11
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan host
switch(config-if)# exit
switch(config)# interface ethernet 1/12
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# exit

switch(config)# interface ethernet 1/11
switch(config-if)# switchport private-vlan host-association 2 3
switch(config-if)# exit
switch(config)# interface ethernet 1/12
switch(config-if)# switchport private-vlan mapping 2 3,4
switch(config-if)# exit

switch(config)# interface vlan 2
switch(config-vlan)# private-vlan mapping 3,4
switch(config-vlan)# exit
switch(config)#
```

## MST Example Configuration

The following example shows how to configure MST:

```
switch# configure terminal
switch(config)# spanning-tree mode mst
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree mst 0-64 priority 24576
switch(config)# spanning-tree mst configuration
switch(config-mst)# name cisco_region_1
switch(config-mst)# revision 2
switch(config-mst)# instance 1 vlan 1-21
switch(config-mst)# instance 2 vlan 22-42
switch(config-mst)# instance 3 vlan 43-63
switch(config-mst)# instance 4 vlan 64-84
switch(config-mst)# instance 5 vlan 85-105
switch(config-mst)# instance 6 vlan 106-126
switch(config-mst)# instance 6 vlan 106-126
switch(config-mst)# instance 7 vlan 127-147
switch(config-mst)# instance 8 vlan 148-168
switch(config-mst)# instance 9 vlan 169-189
switch(config-mst)# instance 10 vlan 190-210
switch(config-mst)# instance 11 vlan 211-231
switch(config-mst)# instance 12 vlan 232-252
switch(config-mst)# instance 13 vlan 253-273
switch(config-mst)# instance 14 vlan 274-294
switch(config-mst)# instance 15 vlan 295-315
```

```
switch(config-mst) # instance 16 vlan 316-336
switch(config-mst) # instance 17 vlan 337-357
switch(config-mst) # instance 18 vlan 358-378
switch(config-mst) # instance 19 vlan 379-399
switch(config-mst) # instance 20 vlan 400-420
switch(config-mst) # instance 21 vlan 421-441
switch(config-mst) # instance 22 vlan 442-462
switch(config-mst) # instance 23 vlan 463-483
switch(config-mst) # instance 24 vlan 484-504
switch(config-mst) # instance 25 vlan 505-525
switch(config-mst) # instance 26 vlan 526-546
switch(config-mst) # instance 27 vlan 547-567
switch(config-mst) # instance 28 vlan 568-588
switch(config-mst) # instance 29 vlan 589-609
switch(config-mst) # instance 30 vlan 610-630
switch(config-mst) # instance 31 vlan 631-651
switch(config-mst) # instance 32 vlan 652-672
switch(config-mst) # instance 33 vlan 673-693
switch(config-mst) # instance 34 vlan 694-714
switch(config-mst) # instance 35 vlan 715-735
switch(config-mst) # instance 36 vlan 736-756
switch(config-mst) # instance 37 vlan 757-777
switch(config-mst) # instance 38 vlan 778-798
switch(config-mst) # instance 39 vlan 799-819
switch(config-mst) # instance 40 vlan 820-840
switch(config-mst) # instance 41 vlan 841-861
switch(config-mst) # instance 42 vlan 862-882
switch(config-mst) # instance 43 vlan 883-903
switch(config-mst) # instance 44 vlan 904-924
switch(config-mst) # instance 45 vlan 925-945
switch(config-mst) # instance 46 vlan 946-966
switch(config-mst) # instance 47 vlan 967-987
switch(config-mst) # instance 48 vlan 988-1008
switch(config-mst) # instance 49 vlan 1009-1029
switch(config-mst) # instance 50 vlan 1030-1050
switch(config-mst) # instance 51 vlan 1051-1071
switch(config-mst) # instance 52 vlan 1072-1092
switch(config-mst) # instance 53 vlan 1093-1113
switch(config-mst) # instance 54 vlan 1114-1134
switch(config-mst) # instance 55 vlan 1135-1155
switch(config-mst) # instance 56 vlan 1156-1176
switch(config-mst) # instance 57 vlan 1177-1197
switch(config-mst) # instance 58 vlan 1198-1218
switch(config-mst) # instance 59 vlan 1219-1239
switch(config-mst) # instance 60 vlan 1240-1260
switch(config-mst) # instance 61 vlan 1261-1281
switch(config-mst) # instance 62 vlan 1282-1302
switch(config-mst) # instance 63 vlan 1303-1323
switch(config-mst) # instance 64 vlan 1324-1344
switch(config-mst) # exit

switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# no shutdown
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit

switch(config)# interface ethernet 3/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# no shutdown
switch(config-if)# spanning-tree guard root
switch(config-if)# exit
switch(config)#
```

## Configuration Examples for STP Extension

The following example shows how to configure the STP extensions:

```
switch# configure terminal
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default

switch(config)# interface ethernet 1/1
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit

switch(config)# interface ethernet 1/2
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)#
```





## CHAPTER 4

# Security Configuration Examples

---

This chapter provides examples for configuring security features.

- [Configuration Example for FIPS, page 16](#)
- [Configuration Examples for AAA, page 16](#)
- [Configuration Example for RADIUS, page 16](#)
- [Configuration Examples for TACACS+, page 16](#)
- [Configuration Example for SSH, page 18](#)
- [Configuration Example for SSH Passwordless File Copy, page 19](#)
- [Configuration Examples for PKI, page 21](#)
- [Configuration Examples for User Accounts and RBAC, page 44](#)
- [Configuration Example for 802.1X, page 45](#)
- [Configuration Example for NAC, page 45](#)
- [Configuration Examples for Cisco TrustSec, page 45](#)
- [Configuration Examples for IP ACLs, page 49](#)
- [Configuration Example for MAC ACLs, page 51](#)
- [Configuration Example for VACLs, page 51](#)
- [Configuration Example for Port Security, page 51](#)
- [Configuration Examples for DHCP, page 51](#)
- [Configuration Examples for DAI, page 52](#)
- [Configuration Example for IP Source Guard, page 58](#)
- [Configuration Examples for Password Encryption, page 58](#)
- [Configuration Example for Keychain Management, page 59](#)
- [Configuration Example for Traffic Storm Control, page 59](#)
- [Configuration Examples for Unicast RPF, page 59](#)

- [Configuration Examples for CoPP, page 60](#)
- [Configuration Examples for Rate Limits, page 63](#)

## Configuration Example for FIPS

The following example shows how to enable FIPS mode:

```
config terminal
fips mode enable
show fips status
exit
copy running-config startup-config
reload
```

## Configuration Examples for AAA

The following example shows how to configure AAA:

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

## Configuration Example for RADIUS

The following example shows how to configure RADIUS:

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
server 10.10.1.1
```

## Configuration Examples for TACACS+

The following example shows how to configure a TACACS+ server host and server group:

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
server 10.10.2.2
```

The following example shows how to configure and use command authorization verification:

```
switch# terminal verify-only
switch# show interface ethernet 7/2 brief
%Success
switch# terminal no verify-only
switch# show interface ethernet 7/2 brief
```

```
-----
Ethernet      VLAN   Type Mode   Status Reason          Speed   Port
Interface                                           Ch #
-----
```

```
Eth7/2      1      eth  access down      SFP not inserted      auto(D) --
```

The following example shows how to enable the cumulative privilege of roles, configure a secret password for privilege level 2, and configure user3 for privilege level 2 authorization:

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret def456 priv-lvl 2
switch(config)# username user3 priv-lvl 2
switch(config)# show privilege
User name: user3
Current privilege level: -2
Feature privilege: Enabled
switch(config)# copy running-config startup-config
switch(config)# exit
```

The following example shows how to change user3 from the priv-2 role to the priv-15 role. After entering the **enable 15** command, the user is prompted to enter the password that was configured by the administrator using the **enable secret** command. Privilege level 15 gives this user network-admin privileges under the enable mode.

```
User Access Verification
login: user3
Password: *****
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright © 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
switch# enable 15
Password: def456
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright © 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch-enable#
```

The following example shows how to permit all users with roles priv-5 and above to execute the **pwd** command:

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)# rule 1 permit command pwd
```

The following example shows how to deny the **show running-config** command to all users with roles below priv-5. First, you must remove the permission to execute this command from the priv-0 role; then you must

permit the command at role priv-5 so that users with roles priv-5 and above have permission to run the command.

```
switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 2 deny command show running-config
switch(config-role)# exit
switch(config)# role name priv-5
switch(config-role)# rule 3 permit command show running-config
switch(config-role)# exit
```

## Configuration Example for SSH

The following example shows how to configure SSH with an OpenSSH key:

### Procedure

**Step 1** Disable the SSH server.

**Example:**

```
switch# configure terminal
switch(config)# no feature ssh
```

**Step 2** Generate an SSH server key.

**Example:**

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
generated rsa key
```

**Step 3** Enable the SSH server.

**Example:**

```
switch(config)# feature ssh
```

**Step 4** Display the SSH server key.

**Example:**

```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr
+MZm99n2U0ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjdDmt923siNiv5aSga60K361r39
HmXL6VgpRVn1XQFiBwn4na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*****
could not retrieve dsa key information
*****
```

**Step 5** Specify the SSH public key in OpenSSH format.

**Example:**

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZ19G+3f1XswK30iW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKu1nIf/DQhum+1JNqJP/eLowb7ubO+1VKRXY/G+1JNlQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5
4Tp1x8=
```

**Step 6** Save the configuration.

**Example:**

```
switch(config)# copy running-config startup-config
```

## Configuration Example for SSH Passwordless File Copy

The following example shows how to copy files from a Cisco NX-OS device to a secure copy (SCP) or secure FTP (SFTP) server without a password:

### Procedure

**Step 1** Generate the SSH public and private keys and store them in the home directory of the Cisco NX-OS device for the specified user.

**Example:**

```
switch# configure terminal
switch(config)# username admin keypair generate rsa
generating rsa key(1024 bits).....
generated rsa key
```

**Step 2** Display the public key for the specified user.

**Example:**

```
switch(config)# show username admin keypair

*****

rsa Keys generated: Thu Jul  9 11:10:29 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcVnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TByPYPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoaJzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****

could not retrieve dsa key information
*****
```

- Step 3** Export the public and private keys from the home directory of the Cisco NX-OS device to the specified bootflash directory.

**Example:**

```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
    951      Jul 09 11:13:59 2009  key_rsa
    221      Jul 09 11:14:00 2009  key_rsa.pub
.
.
```

- Step 4** After copying these two files to another Cisco NX-OS device using the **copy scp** or **copy sftp** command, import them to the home directory of the Cisco NX-OS device.

**Example:**

```
switch(config)# username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username admin keypair
*****

rsa Keys generated: Thu Jul  9 11:10:29 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6r0iztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****

could not retrieve dsa key information
*****
switch(config)#
```

- Step 5** On the SCP or SFTP server, append the public key stored in key\_rsa.pub to the authorized\_keys file.

**Example:**

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

You can now copy files from the Cisco NX-OS device to the server without a password using standard SSH and SCP commands.

- Step 6** (Optional) Repeat this procedure for the DSA keys.
-

# Configuration Examples for PKI

This section shows examples of the tasks that you can use to configure certificates and CRLs on Cisco NX-OS devices using a Microsoft Windows Certificate server.



**Note** You can use any type of certificate server to generate digital certificates. You are not limited to using the Microsoft Windows Certificate server.

## Configuring Certificates on a Cisco NX-OS Device

To configure certificates on a Cisco NX-OS device, follow these steps:

### Procedure

#### Step 1 Configure the device FQDN.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# hostname Device-1
Device-1(config)#
```

#### Step 2 Configure the DNS domain name for the device.

```
Device-1(config)# ip domain-name cisco.com
```

#### Step 3 Create a trust point.

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key:
revokation methods:  crl
```

#### Step 4 Create an RSA key pair for the device.

```
Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes
```

#### Step 5 Associate the RSA key pair to the trust point.

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# rsakeypair myKey
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key: myKey
revokation methods:  crl
```

**Step 6** Download the CA certificate from the Microsoft Certificate Service web interface.

**Step 7** Authenticate the CA that you want to enroll to the trust point.

```
Device-1(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRiljK0ZejanBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk10
MRIwEAYDVQQIEW1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2l2YzY28xEzARBGNVBAStcm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFHhFhbWFuZGt1QGNpc2NvLmNvbTELMakGA1UEBHMCSU4xEjAQBGNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEWVdaXNjbzETMBEG
A1UECXMKbmV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBSIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAGiXT2ASFuUOWq1iDM8rO/41jf8RxxYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoAHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwOC6gLIYqZmlsZTovL1xccc3N1LTA4XEN1cnRfbnJv
bGxcQXBhcm5hJTIwQ0EuY3J5SMBAGCSGAQQBgjcvAQQDAgEAMA0GCSqGSIb3DQEB
BQUAAOEAHv6UQ+8nE399Tww+KaGr0gONIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0cN66zex0EOEfg1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y

Device-1(config)# show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May 3 22:46:37 2005 GMT
notAfter=May 3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

**Step 8** Generate a request certificate to use to enroll with a trust point.

```
Device-1(config)# crypto ca enroll myCA
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: nbv123
The subject name in the certificate will be: Device-1.cisco.com
Include the switch serial number in the subject name? [yes/no]: no
Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
```



```

MIIBqzCCARQCAQAwHDEAMBGA1UEAxMRVnYXNjby5jb20wgZ8wDQYJ
KoZlIhvcNAQEEBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r14lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8orzngShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAGgTzAVBqkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsQGS1b3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVnYXNjby5jb22HBKwWH6IwDQYJ
KoZlIhvcNAQEEBQADgYEAkt60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQl2T3ecgNwe12d15133YBF2bktExiI6U188nTOjg1XMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

```

**Step 9** Request an identity certificate from the Microsoft Certificate Service web interface.

**Step 10** Import the identity certificate.

```

Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEGMB4G
CSqGS1b3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xOzA1BGNVBAITAKlOMRlWEAYD
VQqIEWllYXJuYXRha2ExejaQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2l2
Y28xExZARBGNVBAsTCm5ldHN0b3JhZ2UxExjaQBgNVBAMTCUFwYXJ5SBDQTAeFw0w
NTEeXMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLzE2
Y2l2Y28uY29tMIGfMA0GCSqGS1b3DQEBQUAA4GNADCBiQKBgQC/GNVAcDjQu41C
dQ1WkjkjSICdpLfk5eJSmNCQujGpzcKsZPFxjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYA8rDfz8jMcnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgsl7/Elash9LxLwIDAQABo4ICEZCCAg8wJQYDVR0RAQH/BBsw
GYIRVnYXNjby5jb22HBKwWH6IwHqYDVR0OBByEFKcli+2sspWEfgrR
bhWmlVyo9jngMIHMBGNVHSMegcQwgcGAFCCo8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZlIhvcNAQkBFhFhbWfuZGt1QGNpc2NvLmNvbTELMakGA1UE
BHMCSU4xejaQBgNVBAgTCUthcm5hdGFryTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVdaXNjby5jb22HBKwWH6IwHqYDVR0OBByEFKcli+2sspWEfgrR
cm5hIENBghAFYnKJrLQZ1e9JEiWMrRl6MGsGA1UdHwRkMG1wLqAsocqGKGh0dHA6
Ly9zc2U2MDgVQ2VydEVucm9sb3Bc9BcGFybmElMjBDQS5jcmwwMKAuoCYgKkMzpbGU6
Ly9cXHNzZS0wOFxDZkxJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDcBiGyIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRfbnJvbGwvc3N1
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwoAoYxZmlsZTovL1xccc3N1LTA4
XEN1cnRfbnJvbGwvc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbE7GNLh9xeOTWBNbm24U69ZSuDdcOcuZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsEXREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Device-1(config)# exit
Device-1#

```

**Step 11** Verify the certificate configuration.

**Step 12** Save the certificate configuration to the startup configuration.

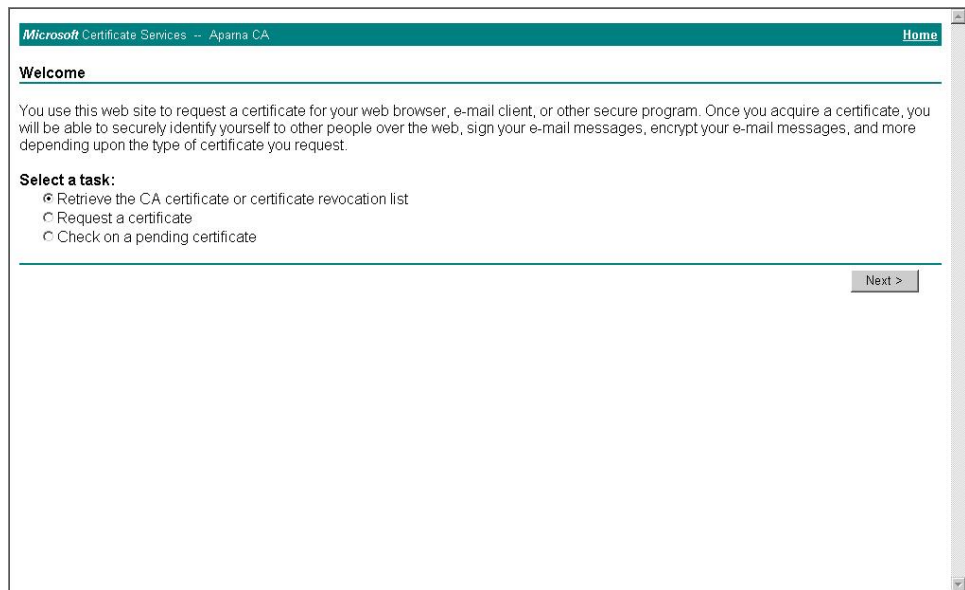
## Downloading a CA Certificate

To download a CA certificate from the Microsoft Certificate Services web interface, follow these steps:

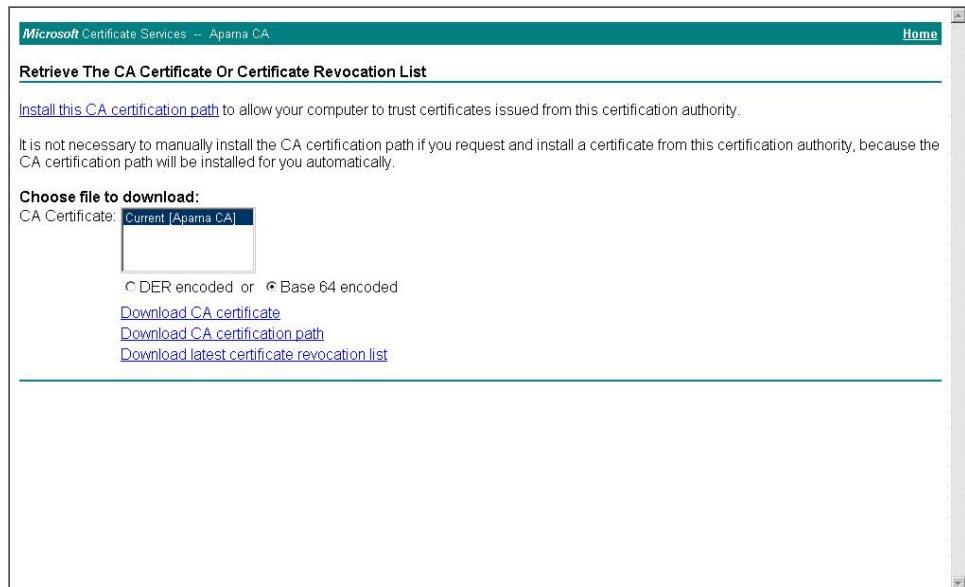
## Procedure

---

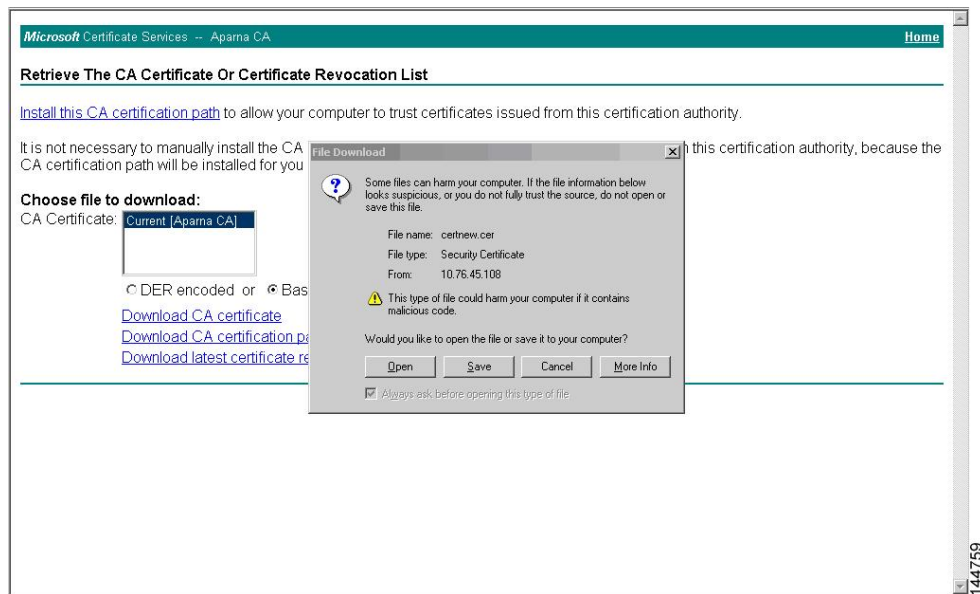
- Step 1** From the Microsoft Certificate Services web interface, click **Retrieve the CA certificate or certificate revocation task** and click **Next**.



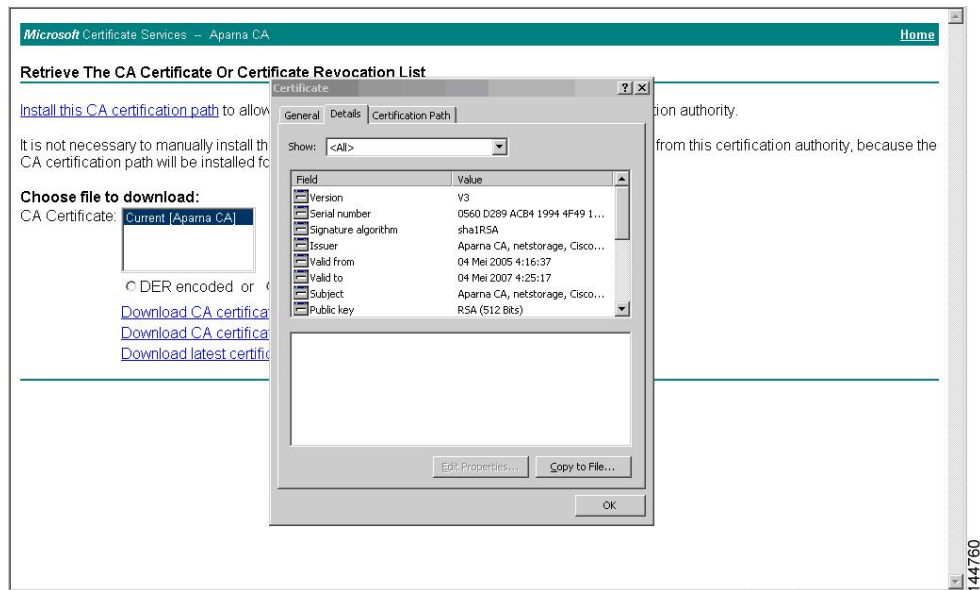
**Step 2** From the display list, choose the CA certificate file to download from the displayed list. Then click **Base 64 encoded** and click **Download CA certificate**.



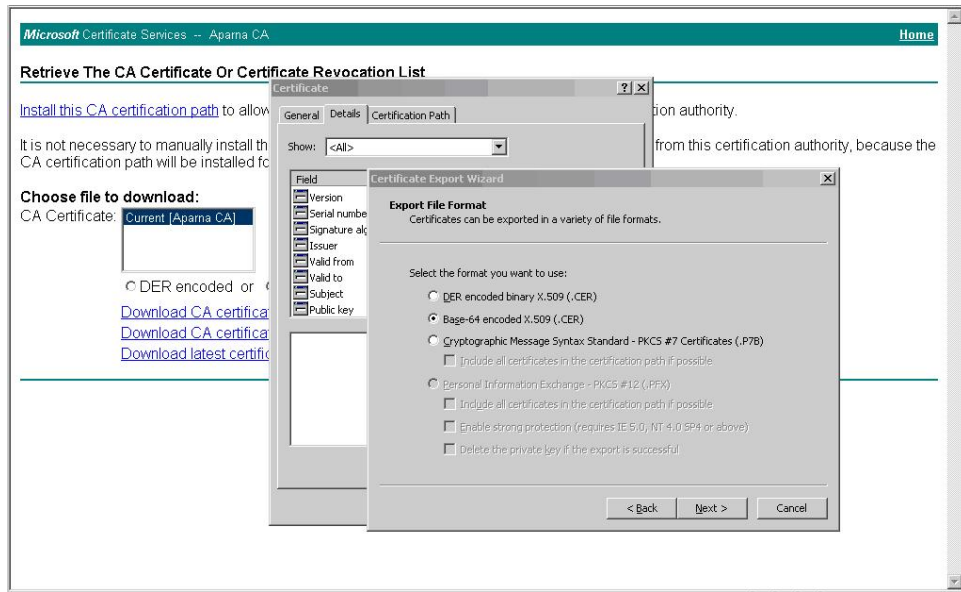
**Step 3** Click **Open** in the File Download dialog box.



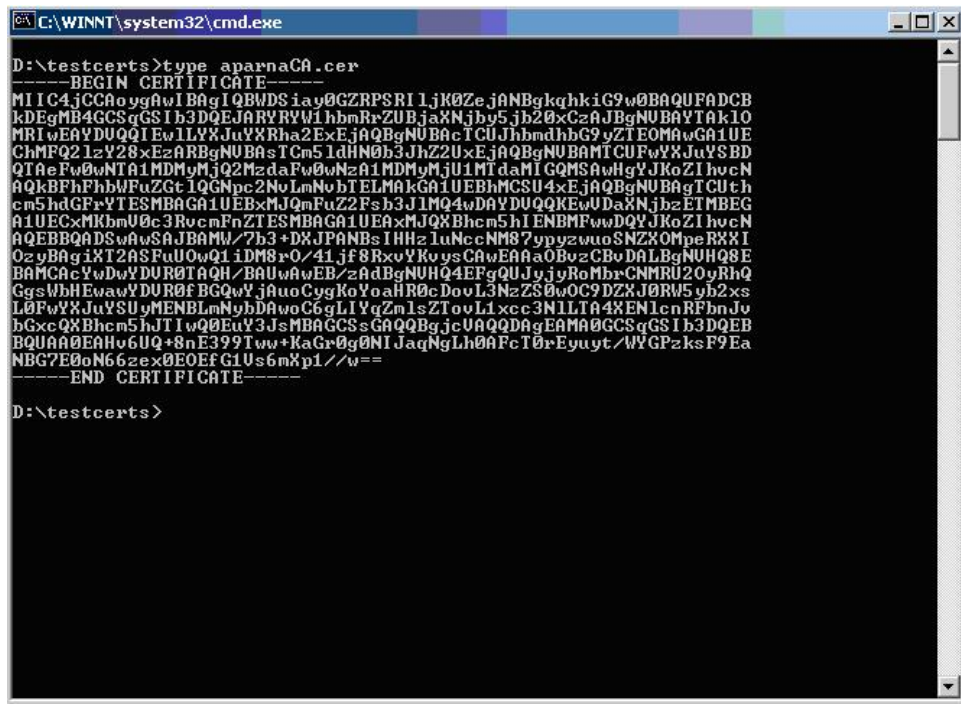
**Step 4** In the Certificate dialog box, click **Copy to File** and click **OK**.



**Step 5** From the Certificate Export Wizard dialog box, choose the **Base-64 encoded X.509 (CER)** and click **Next**.



- Step 6** In the File name: text box on the Certificate Export Wizard dialog box, enter the destination file name and click **Next**.
- Step 7** In the Certificate Export Wizard dialog box, click **Finish**.
- Step 8** Enter the Microsoft Windows **type** command to display the CA certificate stored in Base-64 (PEM) format.



## Requesting an Identity Certificate

To request an identify certificate from a Microsoft Certificate server using a PKCS#12 certificate signing request (CSR), follow these steps:

## Procedure

**Step 1** From the Microsoft Certificate Services web interface, click **Request a certificate** and click **Next**.

Microsoft Certificate Services -- Aparna CA Home

**Welcome**

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

**Select a task:**

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

144765

**Step 2** Click **Advanced request** and click **Next**.

Microsoft Certificate Services -- Aparna CA Home

**Choose Request Type**

Please select the type of request you would like to make:

- User certificate request:
  - Web Browser Certificate
  - E-Mail Protection Certificate
- Advanced request

Next >

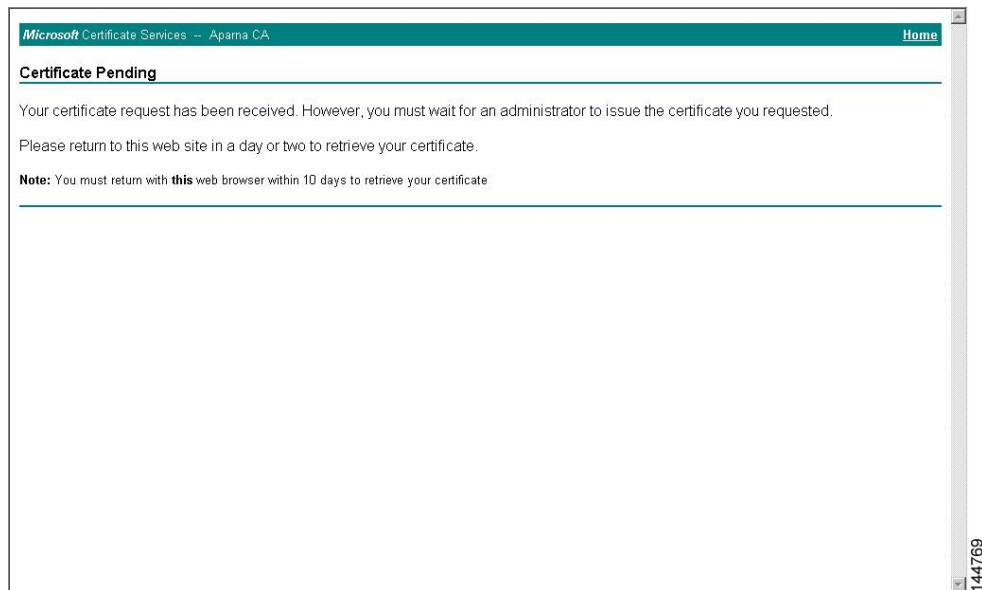
144766

**Step 3** Click **Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file** and click **Next**.

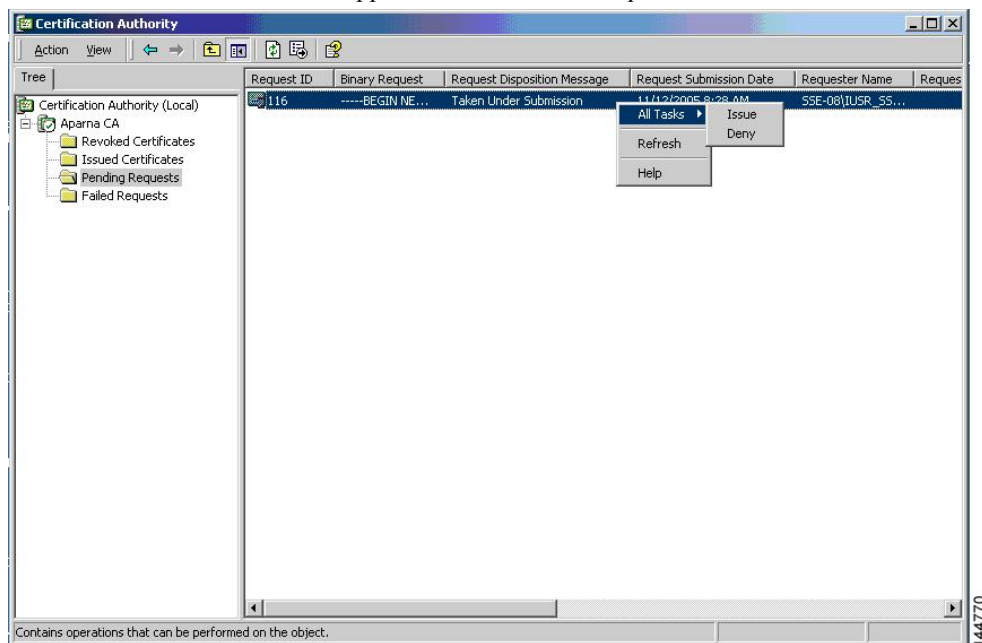
**Step 4** In the Saved Request text box, paste the base64 PKCS#10 certificate request and click **Next**. The certificate request is copied from the Cisco NX-OS device console.

**Step 5** Wait one or two days until the certificate is issued by the CA administrator.

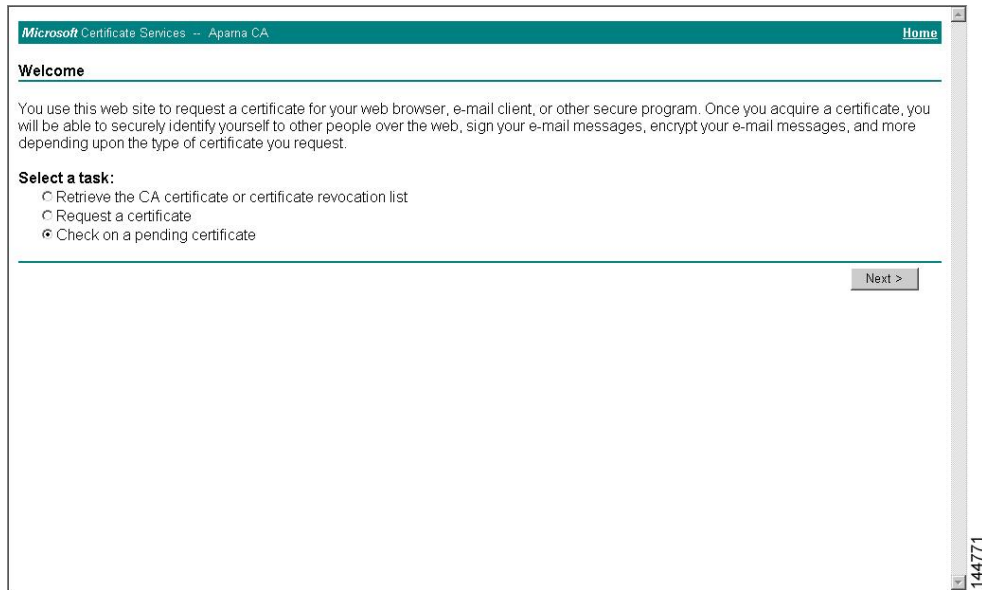




**Step 6** Note that the CA administrator approves the certificate request.



**Step 7** From the Microsoft Certificate Services web interface, click **Check on a pending certificate** and click **Next**.



Microsoft Certificate Services -- Apama CA Home

---

**Welcome**

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

**Select a task:**

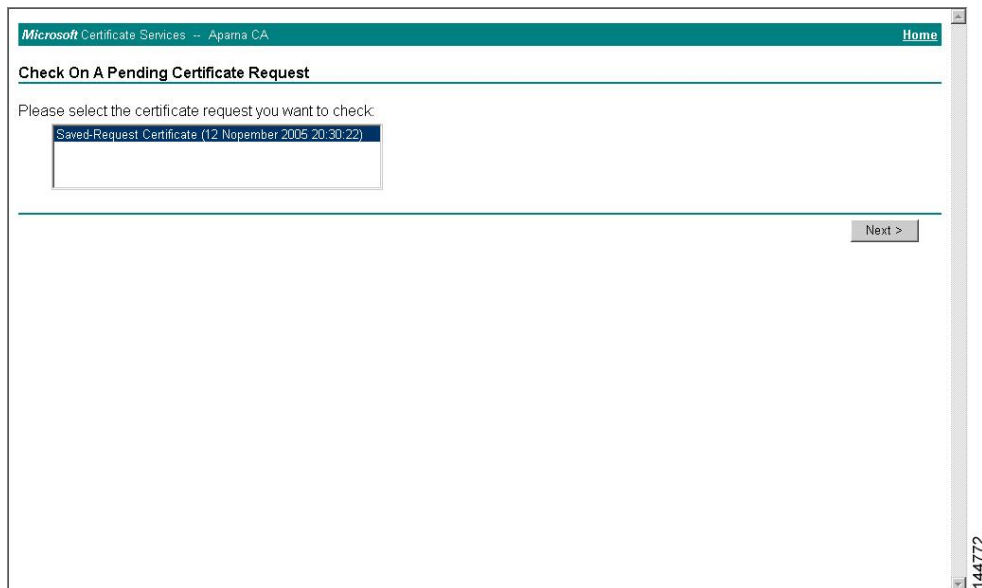
- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

---

Next >

144771

**Step 8** Choose the certificate request that you want to check and click **Next**.



Microsoft Certificate Services -- Apama CA Home

---

**Check On A Pending Certificate Request**

Please select the certificate request you want to check:

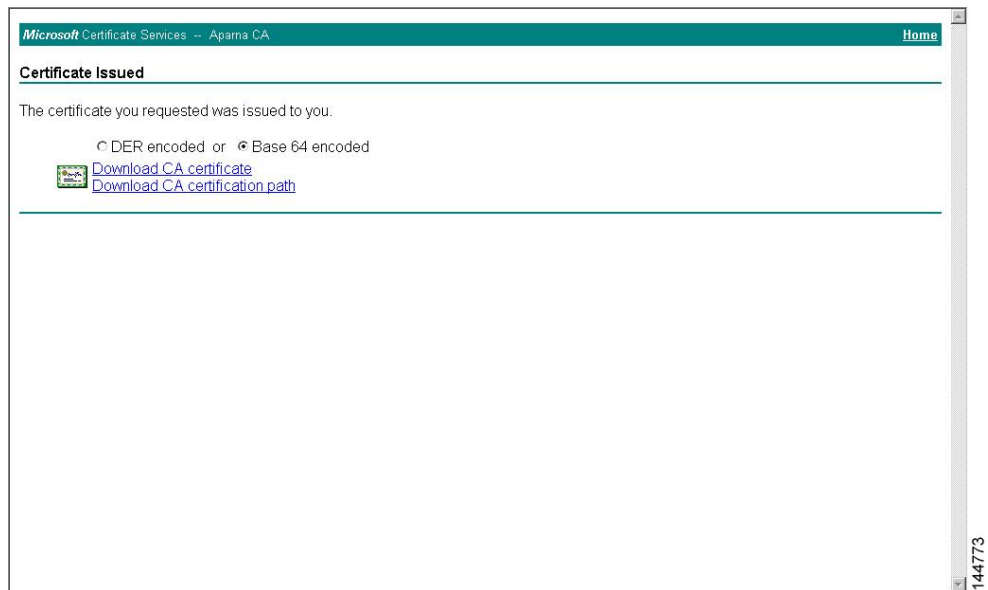
Saved-Request Certificate (12 November 2005 20:30:22)
---

---

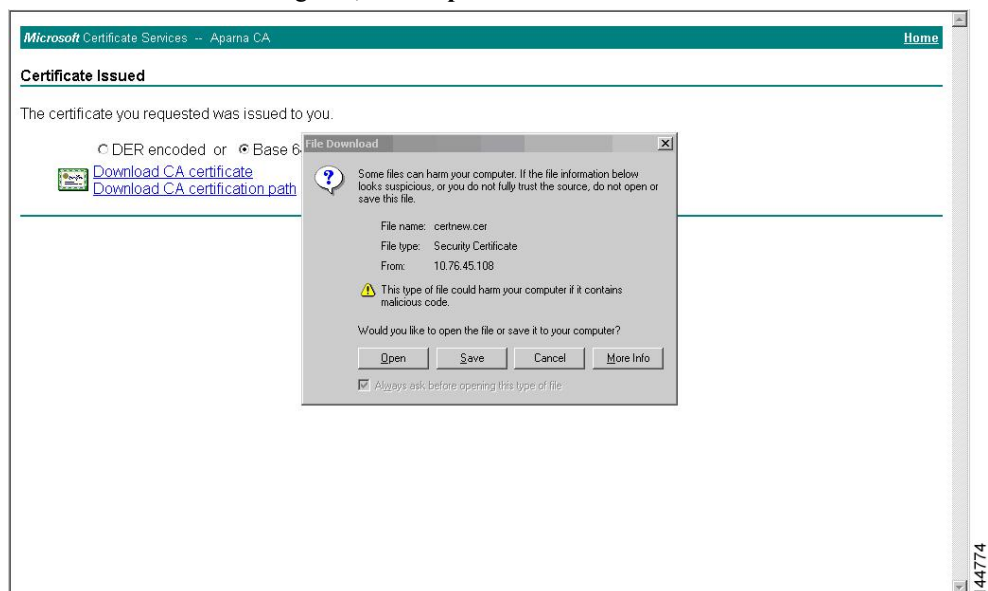
Next >

144772

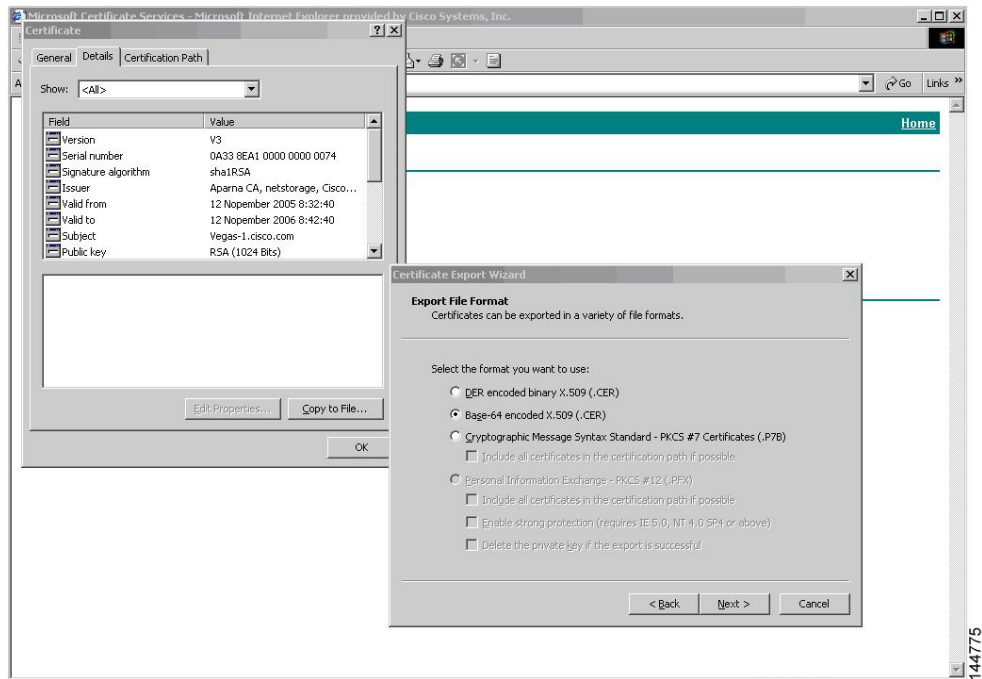
**Step 9** Click **Base 64 encoded** and click **Download CA certificate**.



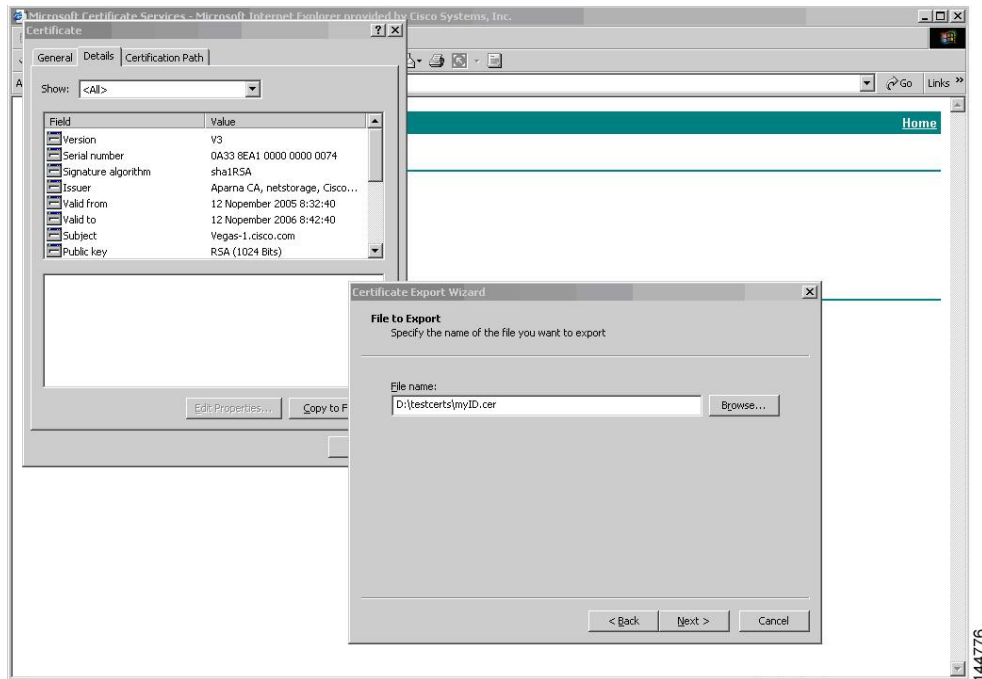
**Step 10** In the File Download dialog box, click **Open**.



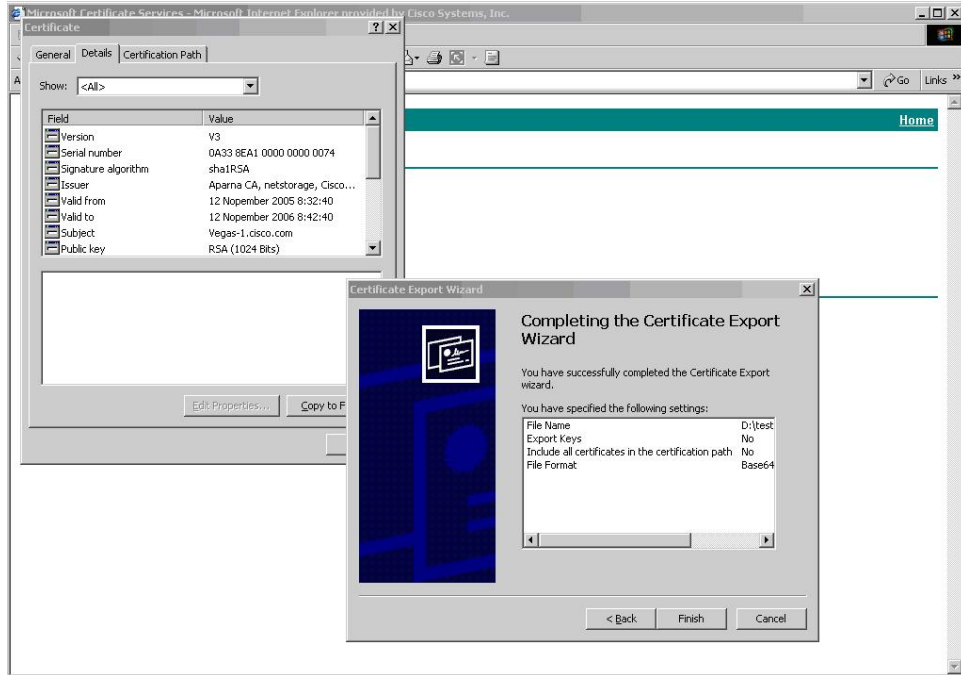
**Step 11** In the Certificate box, click **Details** tab and click **Copy to File....** In the Certificate Export Dialog box, click **Base-64 encoded X.509 (.CER)**, and click **Next**.



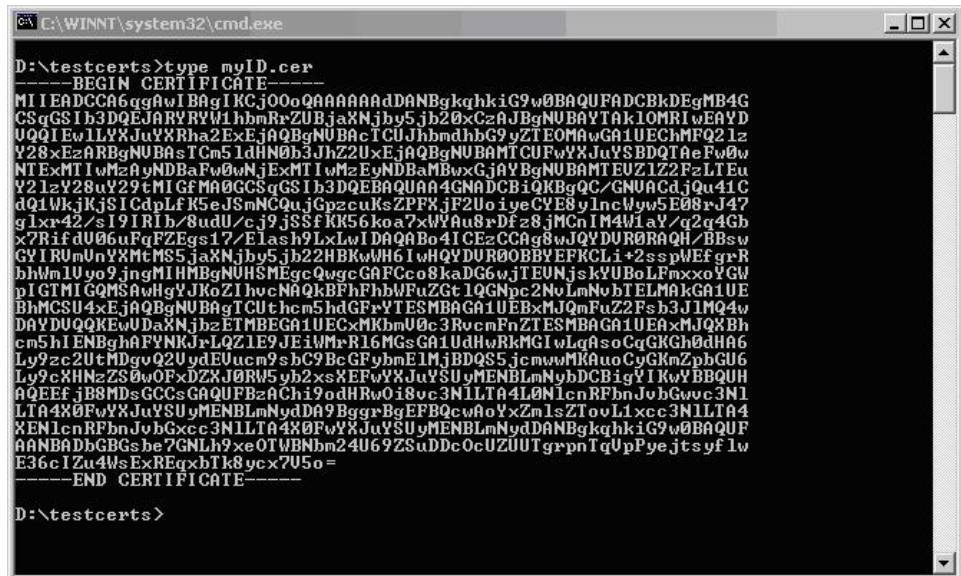
**Step 12** In the File name: text box on the Certificate Export Wizard dialog box, enter the destination file name and click **Next**.



**Step 13** Click **Finish**.



**Step 14** Enter the Microsoft Windows **type** command to display the identity certificate in base64-encoded format.

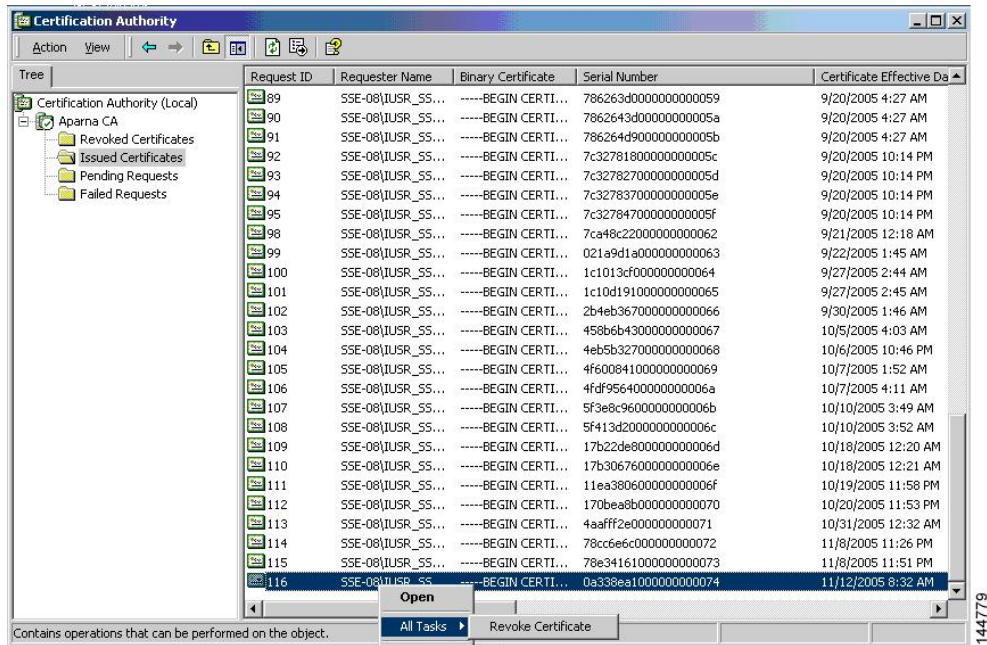


## Revoking a Certificate

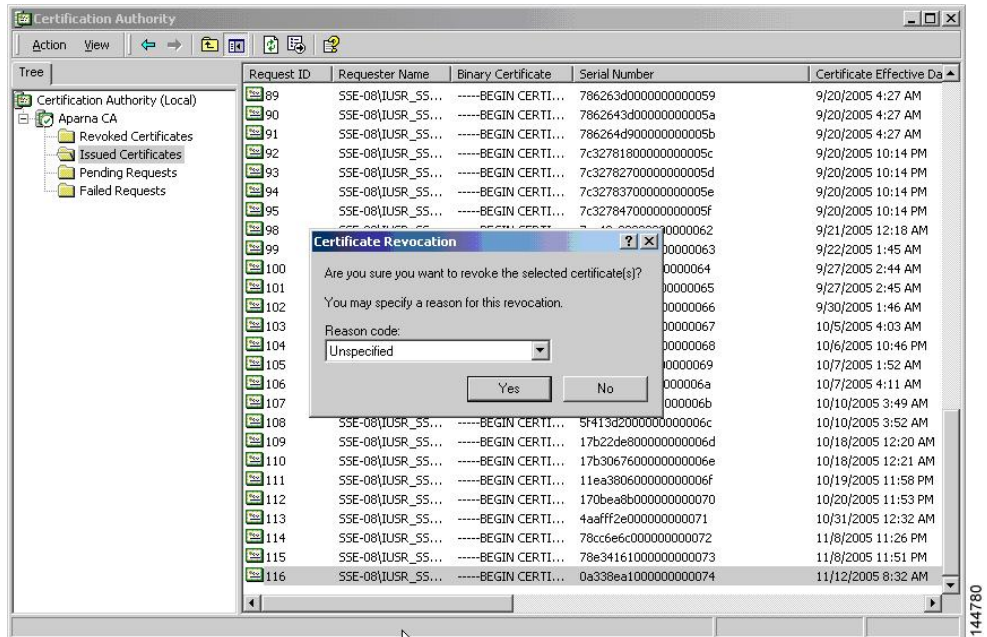
To revoke a certificate using the Microsoft CA administrator program, follow these steps:

## Procedure

- Step 1** From the Certification Authority tree, click **Issued Certificates** folder. From the list, right-click the certificate that you want to revoke.
- Step 2** Choose **All Tasks > Revoke Certificate**.



- Step 3** From the Reason code drop-down list, choose a reason for the revocation and click **Yes**.



- Step 4** Click the **Revoked Certificates** folder to list and verify the certificate revocation.



The screenshot shows the Microsoft Certification Authority console. The left pane displays the tree structure: Certification Authority (Local) > Aparna CA > Issued Certificates. The main pane shows a list of certificates with the following columns: Request ID, Requester Name, Binary Certificate, Serial Number, and Certificate Effective Date. The list contains 20 entries, each with a red 'X' icon in the Request ID column, indicating that the certificates are expired or revoked.

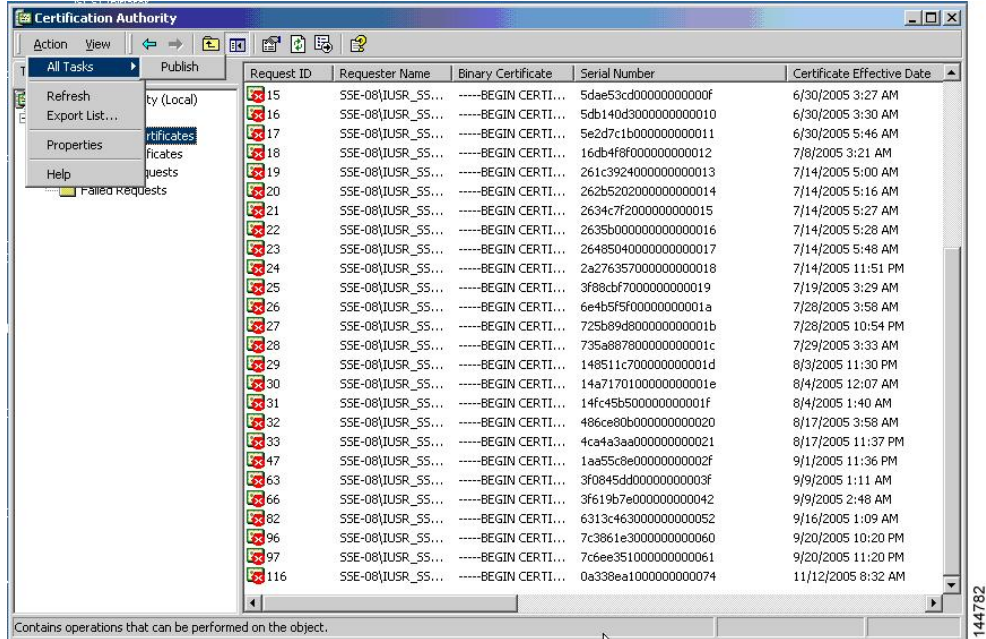
Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective Date
15	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5dae53cd0000000000f	6/30/2005 3:27 AM
16	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5db140d300000000010	6/30/2005 3:30 AM
17	SSE-08\IUSR_SS...	-----BEGIN CERTI...	5e2d7c1b00000000011	6/30/2005 5:46 AM
18	SSE-08\IUSR_SS...	-----BEGIN CERTI...	16db4f8f00000000012	7/8/2005 3:21 AM
19	SSE-08\IUSR_SS...	-----BEGIN CERTI...	261c392400000000013	7/14/2005 5:00 AM
20	SSE-08\IUSR_SS...	-----BEGIN CERTI...	262b520200000000014	7/14/2005 5:16 AM
21	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2634c7f200000000015	7/14/2005 5:27 AM
22	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2635b00000000000016	7/14/2005 5:28 AM
23	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2648504000000000017	7/14/2005 5:48 AM
24	SSE-08\IUSR_SS...	-----BEGIN CERTI...	2a27635700000000018	7/14/2005 11:51 PM
25	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f88cbf700000000019	7/19/2005 3:29 AM
26	SSE-08\IUSR_SS...	-----BEGIN CERTI...	6e4b5f5f0000000001a	7/28/2005 3:58 AM
27	SSE-08\IUSR_SS...	-----BEGIN CERTI...	725b89d80000000001b	7/28/2005 10:54 PM
28	SSE-08\IUSR_SS...	-----BEGIN CERTI...	735a88780000000001c	7/29/2005 3:33 AM
29	SSE-08\IUSR_SS...	-----BEGIN CERTI...	148511c70000000001d	8/3/2005 11:30 PM
30	SSE-08\IUSR_SS...	-----BEGIN CERTI...	148717010000000001e	8/4/2005 12:07 AM
31	SSE-08\IUSR_SS...	-----BEGIN CERTI...	14fc45b50000000001f	8/4/2005 1:40 AM
32	SSE-08\IUSR_SS...	-----BEGIN CERTI...	486ce80b00000000020	8/17/2005 3:58 AM
33	SSE-08\IUSR_SS...	-----BEGIN CERTI...	4ca4a3aa00000000021	8/17/2005 11:37 PM
47	SSE-08\IUSR_SS...	-----BEGIN CERTI...	1aa55c8e0000000002f	9/1/2005 11:36 PM
63	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f0845dd0000000003f	9/9/2005 1:11 AM
66	SSE-08\IUSR_SS...	-----BEGIN CERTI...	3f619b7e00000000042	9/9/2005 2:48 AM
82	SSE-08\IUSR_SS...	-----BEGIN CERTI...	6313c46300000000052	9/16/2005 1:09 AM
96	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c3861e300000000060	9/20/2005 10:20 PM
97	SSE-08\IUSR_SS...	-----BEGIN CERTI...	7c6ee35100000000061	9/20/2005 11:20 PM
116	SSE-08\IUSR_SS...	-----BEGIN CERTI...	0a338ea100000000074	11/12/2005 8:32 AM

## Generating and Publishing the CRL

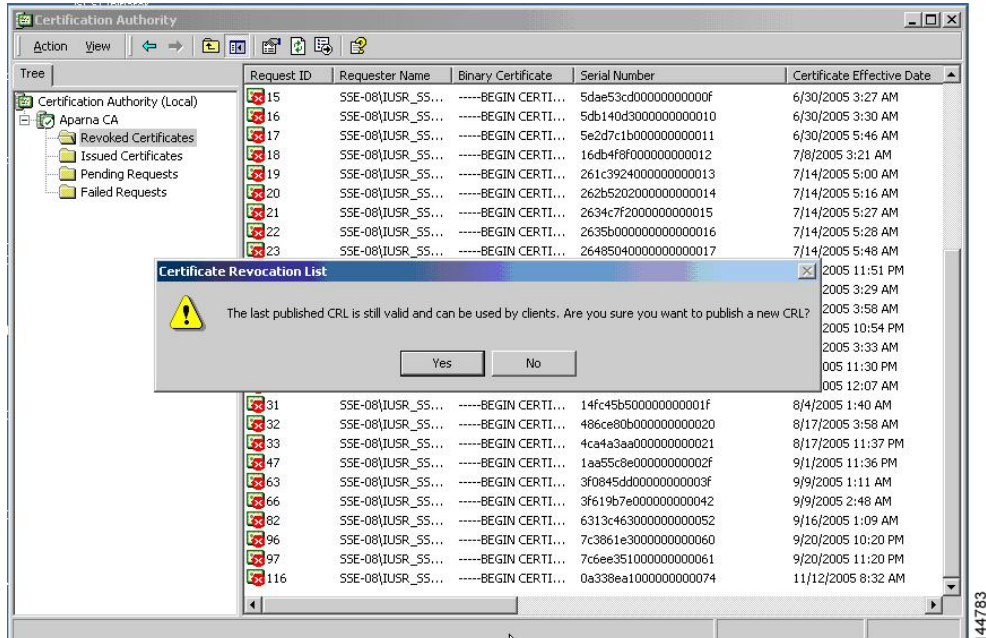
To generate and publish the CRL using the Microsoft CA administrator program, follow these steps:

## Procedure

**Step 1** From the Certification Authority screen, choose **Action > All Tasks > Publish**.



**Step 2** In the Certificate Revocation List dialog box, click **Yes** to publish the latest CRL.





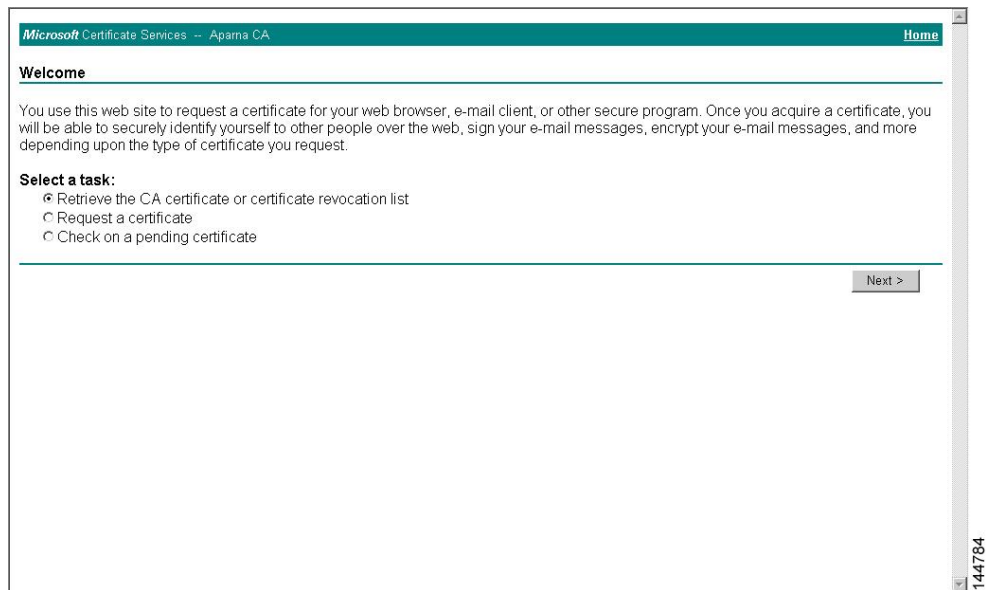
## Downloading the CRL

To download the CRL from the Microsoft CA website, follow these steps:

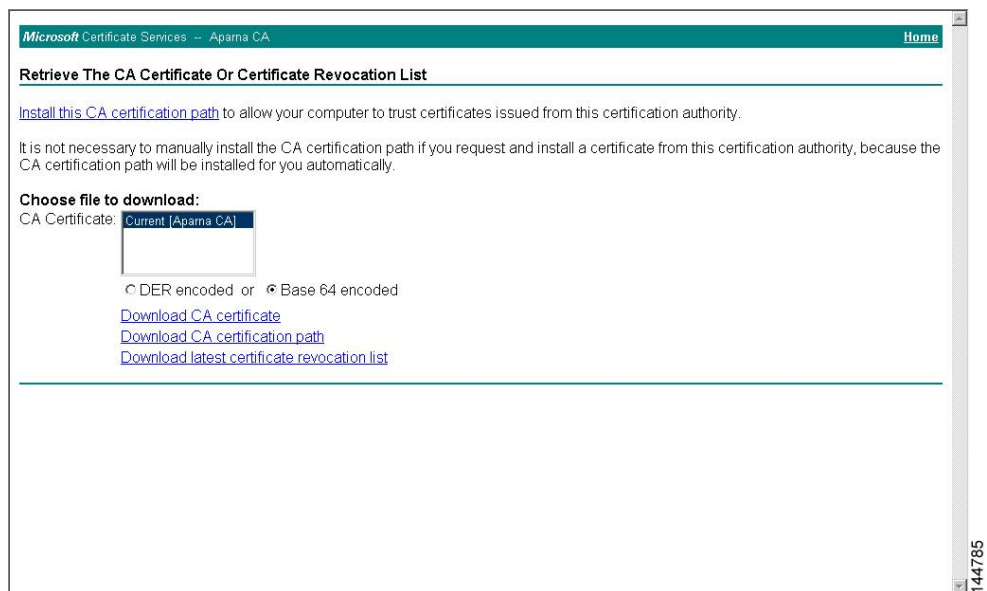
### Procedure

---

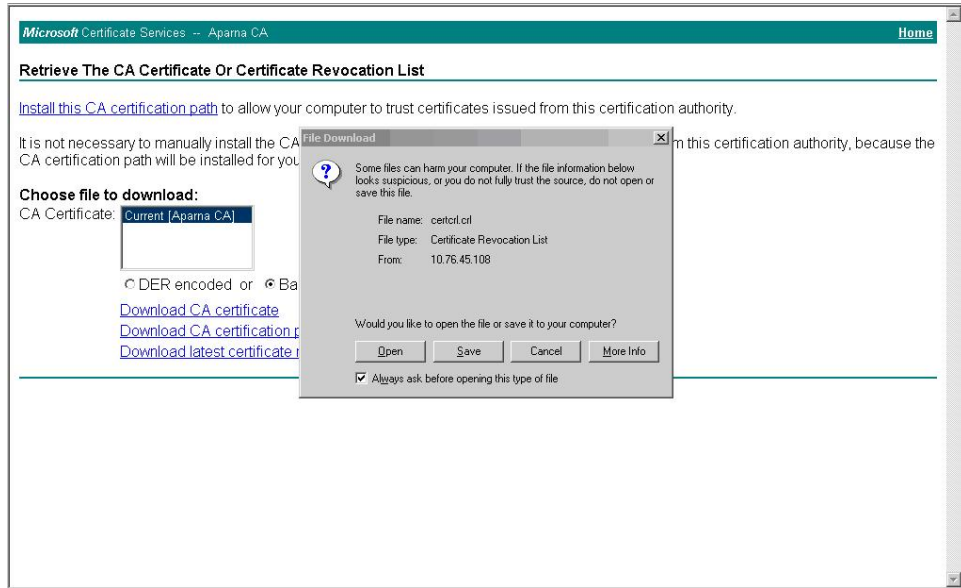
- Step 1** From the Microsoft Certificate Services web interface, click **Retrieve the CA certificate or certificate revocation list** and click **Next**.



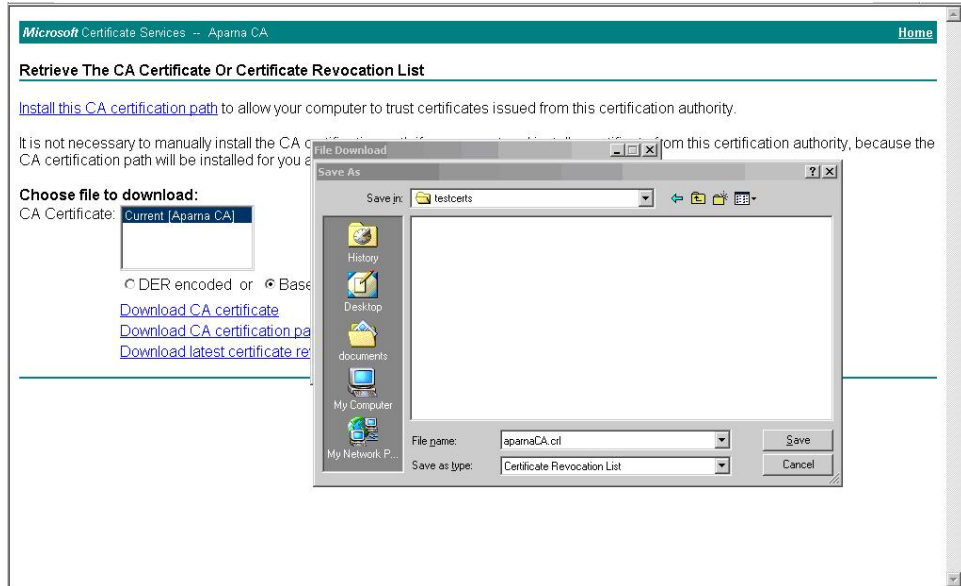
**Step 2** Click **Download latest certificate revocation list**.



**Step 3** In the File Download dialog box, click **Save**.



**Step 4** In the Save As dialog box, enter the destination file name and click **Save**.



**Step 5** Enter the Microsoft Windows **type** command to display the CRL.



**Example:**

```

Device-1(config)# show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
  Last Update: Nov 12 04:36:04 2005 GMT
  Next Update: Nov 19 16:56:04 2005 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
      1.3.6.1.4.1.311.21.1:
        ...
  Revoked Certificates:
    Serial Number: 611B09A1000000000002
      Revocation Date: Aug 16 21:52:19 2005 GMT
    Serial Number: 4CDE464E000000000003
      Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B42000000000004
      Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC2000000000005
      Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC000000000006
      Revocation Date: Jun 8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF000000000007
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B1116000000000008
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A80230000000000009
      Revocation Date: Jun 27 23:47:06 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          CA Compromise
    Serial Number: 5349AD4600000000000A
      Revocation Date: Jun 27 23:47:22 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          CA Compromise
    Serial Number: 53BD173C00000000000B
      Revocation Date: Jul 4 18:04:01 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Certificate Hold
    Serial Number: 591E7ACE00000000000C
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E00000000000D
      Revocation Date: Jun 29 22:07:25 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Key Compromise
    Serial Number: 5DAB771300000000000E
      Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD00000000000F
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D3000000000010
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B000000000011
      Revocation Date: Jul 6 21:12:10 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Cessation Of Operation
    Serial Number: 16DB4F8F000000000012
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C3924000000000013
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 262B5202000000000014

```

```

    Revocation Date: Jul 14 00:33:10 2005 GMT
  Serial Number: 2634C7F2000000000015
    Revocation Date: Jul 14 00:32:45 2005 GMT
  Serial Number: 2635B000000000000016
    Revocation Date: Jul 14 00:31:51 2005 GMT
  Serial Number: 26485040000000000017
    Revocation Date: Jul 14 00:32:25 2005 GMT
  Serial Number: 2A276357000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 3F88CBF7000000000019
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 6E4B5F5F00000000001A
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 725B89D800000000001B
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 735A887800000000001C
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 148511C700000000001D
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 14A7170100000000001E
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 14FC45B500000000001F
    Revocation Date: Aug 17 18:30:42 2005 GMT
  Serial Number: 486CE80B000000000020
    Revocation Date: Aug 17 18:30:43 2005 GMT
  Serial Number: 4CA4A3AA000000000021
    Revocation Date: Aug 17 18:30:43 2005 GMT
  Serial Number: 1AA55C8E00000000002F
    Revocation Date: Sep  5 17:07:06 2005 GMT
  Serial Number: 3F0845DD00000000003F
    Revocation Date: Sep  8 20:24:32 2005 GMT
  Serial Number: 3F619B7E000000000042
    Revocation Date: Sep  8 21:40:48 2005 GMT
  Serial Number: 6313C463000000000052
    Revocation Date: Sep 19 17:37:18 2005 GMT
  Serial Number: 7C3861E3000000000060
    Revocation Date: Sep 20 17:52:56 2005 GMT
  Serial Number: 7C6EE351000000000061
    Revocation Date: Sep 20 18:52:30 2005 GMT
  Serial Number: 0A338EA1000000000074  <-- Revoked identity certificate
    Revocation Date: Nov 12 04:34:42 2005 GMT
  Signature Algorithm: sha1WithRSAEncryption
    0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
    44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
    29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
    1a:9f:1a:49:b7:9c:58:24:d7:72

```

**Note** The identity certificate for the device that was revoked (serial number 0A338EA1000000000074) is listed at the end.

## Configuration Examples for User Accounts and RBAC

The following example shows how to configure a user role:

```

role name User-role-A
  rule 3 permit read-write feature l2nac
  rule 2 permit read-write feature dot1x
  rule 1 deny command clear *

```

The following example shows how to create a user role that can configure an interface to enable and show HSRP and show GLBP:

```

role name iftest
  rule 1 permit command config t; interface *; hsrp *
  rule 2 permit read-write feature hsrp

```

```
rule 3 permit read feature glbp
```

In the above example, rule 1 allows you to configure HSRP on an interface, rule 2 allows you to configure the **config hsrp** commands and enable the exec-level **show** and **debug** commands for HSRP, and rule 3 allows you to enable the exec-level **show** and **debug glbp** commands.

The following example shows how to configure a user role that can configure only a specific interface:

```
role name Int_Eth2-3_only
  rule 1 permit command configure terminal; interface *
  interface policy deny
    permit interface Ethernet2/3
```

The following example shows how to configure a user role feature group:

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature dot1x
  feature aaa
  feature l2nac
  feature acl
  feature access-list
```

The following example shows how to configure a user account:

```
username user1 password A1s2D4f5 role User-role-A
```

## Configuration Example for 802.1X

The following example shows how to configure 802.1X:

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
  dot1x port-control auto
```



### Note

---

Repeat the **dot1x port-control auto** command for all interfaces that require 802.1X authentication.

---

## Configuration Example for NAC

The following example shows how to configure NAC:

```
feature eou
aaa authentication eou default group radius
mac access-list macacl-01
  10 permit any any 0x100
interface Ethernet8/1
  mac access-group macacl-01
```

## Configuration Examples for Cisco TrustSec

This section provides configuration examples for Cisco TrustSec.

## Enabling Cisco TrustSec

The following example shows how to enable Cisco TrustSec:

```
feature dot1x
feature cts
cts device-id device1 password Cisco321
```

## Configuring AAA for Cisco TrustSec on a Seed Cisco NX-OS Device

The following example shows how to configure AAA for Cisco TrustSec on the seed Cisco NX-OS device:

```
radius-server host 10.10.1.1 key Cisco123 pac
aaa group server radius Rad1
  server 10.10.1.1
  use-vrf management
aaa authentication dot1x default group Rad1
aaa authorization cts default group Rad1
```

## Enabling Cisco TrustSec Authentication on an Interface

The following example shows how to enable Cisco TrustSec authentication with a clear text password on an interface:

```
interface ethernet 2/1
  cts dot1x
  shutdown
  no shutdown
```

## Configuring Cisco TrustSec Authentication in Manual Mode

The following example shows how to configure Cisco TrustSec authentication in manual mode static policy on an interface:

```
interface ethernet 2/1
  cts manual
  sap pmk abcdef modelist gmac
  policy static sgt 0x20
```

The following example shows how to configure Cisco TrustSec authentication in manual mode dynamic policy on an interface:

```
interface ethernet 2/2
  cts manual
  policy dynamic identity device2
```



## Configuring Cisco TrustSec Role-Based Policy Enforcement for the default VRF

The following example shows how to enable Cisco TrustSec role-based policy enforcement for the default VRF:

```
cts role-based enforcement
```

## Configuring Cisco TrustSec Role-Based Policy Enforcement for a Nondefault VRF

The following example shows how to enable Cisco TrustSec role-based policy enforcement for a nondefault VRF:

```
vrf context test
  cts role-based enforcement
```

## Configuring Cisco TrustSec Role-Based Policy Enforcement for a VLAN

The following example shows how to enable Cisco TrustSec role-based policy enforcement for a VLAN:

```
vlan 10
  cts role-based enforcement
```

## Configuring IPv4 Address to SGACL SGT Mapping for the Default VRF

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for the default VRF:

```
cts role-based sgt-map 10.1.1.1 20
```

## Configuring IPv4 Address to SGACL SGT Mapping for a Nondefault VRF

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for a nondefault VRF:

```
vrf context test
  cts role-based sgt-map 30.1.1.1 30
```

## Configuring IPv4 Address to SGACL SGT Mapping for a VLAN

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for a VLAN:

```
vlan 10
  cts role-based sgt-map 20.1.1.1 20
```

## Manually Configuring Cisco TrustSec SGACLs

The following example shows how to manually configure Cisco TrustSec SGACLs:

```
cts role-based access-list abcd
  permit icmp
cts role-based sgt 10 dgt 20 access-list abcd
```

The following example shows how to enable RBACL logging:

```
cts role-based access-list RBACL1
deny tcp src eq 1111 dest eq 2222 log
cts role-based sgt 10 dgt 20 access-list RBACL1
cts role-based sgt-map 1.1.1.1 10
cts role-based sgt-map 1.1.1.2 20
```

The above configuration generates the following ACLLOG syslog:

```
%ACLLOG-6-ACLLOG_FLOW_INTERVAL: SGT: 10, Source IP: 1.1.1.1, Destination IP: 1.1.1.2, Source
Port: 1111, Destination Port: 2222, Source Interface: Ethernet4/1, Protocol: tcp, Hit-count
= 2
```



### Note

The ACLLOG syslog does not contain the destination group tag (DGT) information of the matched RBACL policy. You can find this information by looking up the IP-SGT mapping of the destination IP address in the log message and then entering the **show cts role-based sgt-map** command.

The following example shows how to enable and display RBACL statistics:

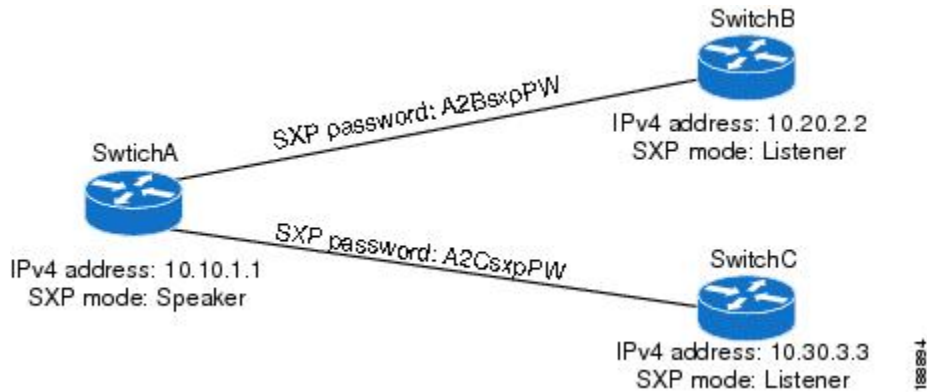
```
cts role-based counters enable
show cts role-based counters sgt 10 dgt 20

RBACL policy counters enabled
sgt: 10 dgt: 20 [180]
rbacl test1:
deny tcp src eq 1111 dest eq 2222 [75]
deny tcp src eq 2222 dest eq 3333 [25]
rbacl test2:
deny udp src eq 1111 dest eq 2222 [30]
deny udp src eq 2222 dest eq 3333 [50]
```

## Manually Configuring SXP Peer Connections

This figure shows an example of SXP peer connections over the default VRF.

**Figure 1: Example SXP Peer Connections**



The following example shows how to configure the SXP peer connections on SwitchA:

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.20.2.2 password required A2BsxpPW mode listener
cts sxp connection peer 10.30.3.3 password required A2CsxpPW mode listener
```

The following example shows how to configure the SXP peer connection on SwitchB:

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2BsxpPW mode speaker
```

The following example shows how to configure the SXP peer connection on SwitchC:

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2CsxpPW mode speaker
```

## Configuration Examples for IP ACLs

The following example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to Ethernet interface 2/1, which is a Layer 2 interface:

```
ip access-list acl-01
 permit ip 192.168.2.0/24 any
interface ethernet 2/1
 ip port access-group acl-01 in
```

The following example shows how to create an IPv6 ACL named `acl-120` and apply it as a router ACL to Ethernet interface `2/3`, which is a Layer 3 interface:

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

The following example shows how to create a VTY ACL named `single-source` and apply it on input IP traffic over the VTY line. This ACL allows all TCP traffic through and drops all other IP traffic:

```
ip access-list single-source
  permit tcp 192.168.7.5/24 any
  exit
line vty
  ip access-class single-source in
  show ip access-lists
```

The following example shows how to enable ACL capture in the default VDC and configure a destination for ACL capture packets:

```
hardware access-list capture
  monitor session 1 type acl-capture
  destination interface ethernet 2/1
  no shut
  exit
  show ip access-lists capture session 1
```

The following example shows how to enable a capture session for an ACL's access control entries (ACEs) and then apply the ACL to an interface:

```
ip access-list acl1
  permit tcp any any capture session 1
  exit
interface ethernet 1/11
  ip access-group acl1 in
  no shut
  show running-config aclmgr
```

The following example shows how to apply an ACL with capture session access control entries (ACEs) to a VLAN:

```
vlan access-map acl-vlan-first
  match ip address acl-ipv4-first
  match mac address acl-mac-first
  action forward
  statistics per-entry
  vlan filter acl-vlan-first vlan-list 1
  show running-config vlan 1
```

The following example shows how to enable a capture session for the whole ACL and then apply the ACL to an interface:

```
ip access-list acl2
  capture session 2
  exit
interface ethernet 7/1
  ip access-group acl1 in
  no shut
  show running-config aclmgr
```

## Configuration Example for MAC ACLs

The following example shows how to create a MAC ACL named `acl-mac-01` and apply it to Ethernet interface `2/1`, which is a Layer 2 interface in this example:

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface ethernet 2/1
  mac port access-group acl-mac-01
```

## Configuration Example for VACLs

The following example shows how to configure a VACL to forward traffic permitted by a MAC ACL named `acl-mac-01` and how to apply the VACL to VLANs 50 through 82.

```
conf t
vlan access-map acl-mac-map
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

## Configuration Example for Port Security

The following example shows a port security configuration for the Ethernet `2/1` interface with VLAN and interface maximums for secure addresses. In this example, the interface is a trunk port. Additionally, the violation action is set to Restrict.

```
feature port-security
interface Ethernet 2/1
  switchport
  switchport port-security
  switchport port-security maximum 10
  switchport port-security maximum 7 vlan 10
  switchport port-security maximum 3 vlan 20
  switchport port-security violation restrict
```

## Configuration Examples for DHCP

This example shows how to enable DHCP snooping on two VLANs, with Option 82 support enabled and Ethernet interface `2/5` trusted because the DHCP server is connected to that interface:

```
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet 2/5
  ip dhcp snooping trust
  ip dhcp snooping vlan 1
  ip dhcp snooping vlan 50
```

This example shows how to enable the DHCP relay agent and configure the DHCP server IP address for Ethernet interface `2/3`, where the DHCP server IP address is `10.132.7.120` and the DHCP server is in the VRF named `red`:

```
feature dhcp
ip dhcp snooping
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
```

```
interface Ethernet 2/3
 ip dhcp relay address 10.132.7.120 use-vrf red
```

This example shows how to enable and use the DHCP smart relay agent. In this example, the switch forwards the DHCP broadcast packets received on Ethernet interface 2/2 to the DHCP server (10.55.11.3), inserting 192.168.100.1 in the giaddr field. If the DHCP server has a pool configured for the 192.168.100.0/24 network, it responds. If the server does not respond, the switch sends two more requests using 192.168.100.1 in the giaddr field. If the switch still does not receive a response, it starts using 172.16.31.254 in the giaddr field instead.

```
feature dhcp
ip dhcp snooping
ip dhcp relay
ip dhcp smart-relay global

interface Ethernet 2/2
 ip address 192.168.100.1/24
 ip address 172.16.31.254/24 secondary
 ip dhcp relay address 10.55.11.3
```

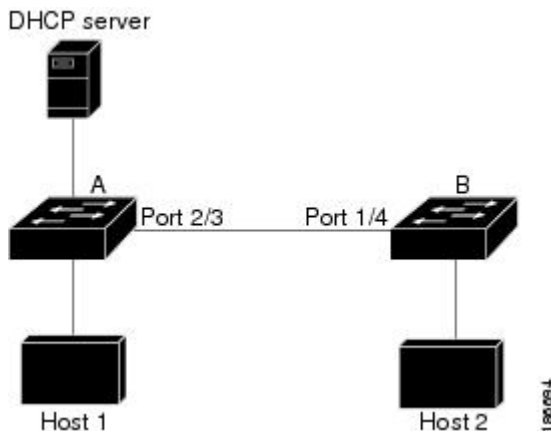
## Configuration Examples for DAI

### Example 1 Two Devices Support DAI

These procedures show how to configure DAI when two devices support DAI.

This figure shows the network configuration for this example. Host 1 is connected to device A, and Host 2 is connected to device B. Both devices are running DAI on VLAN 1 where the hosts are located. A DHCP server is connected to device A. Both hosts acquire their IP addresses from the same DHCP server. Device A has the bindings for Host 1 and Host 2, and device B has the binding for Host 2. Device A Ethernet interface 2/3 is connected to the device B Ethernet interface 1/4.

**Figure 2: Two Devices Supporting DAI**



DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically-assigned IP addresses.

- This configuration does not work if the DHCP server is moved from device A to a different location.

- To ensure that this configuration does not compromise security, configure Ethernet interface 2/3 on device A and Ethernet interface 1/4 on device B as trusted.

## Configuring Device A

To enable DAI and configure Ethernet interface 2/3 on device A as trusted, follow these steps:

### Procedure

**Step 1** While logged into device A, verify the connection between device A and device B.

#### Example:

```
switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce   Hldtme   Capability   Platform     Port ID
switchB           Ethernet2/3     177      R S I       WS-C2960-24TC Ethernet1/4
switchA#
```

**Step 2** Enable DAI on VLAN 1 and verify the configuration.

#### Example:

```
switchA# config t
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----
Configuration      : Enabled
Operation State    : Active
switchA(config)#
```

**Step 3** Configure Ethernet interface 2/3 as trusted.

#### Example:

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3
Interface      Trust State      Rate (pps)      Burst Interval
-----
Ethernet2/3    Trusted          15              5
```

**Step 4** Verify the bindings.

#### Example:

```
switchA# show ip dhcp snooping binding
MacAddress      IpAddress      LeaseSec   Type          VLAN   Interface
-----
00:60:0b:00:12:89 10.0.0.1      0          dhcp-snooping 1      Ethernet2/3
switchA#
```

**Step 5** Check the statistics before and after DAI processes any packets.

**Example:**

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 0
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

If Host 1 sends out two ARP requests with an IP address of 10.0.0.1 and a MAC address of 0002.0002.0002, both requests are permitted, shown as follows:

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 2
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

If Host 1 tries to send an ARP request with an IP address of 10.0.0.3, the packet is dropped and an error message is logged.

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1. ([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

The statistics display as follows:

```
switchA# show ip arp inspection statistics vlan 1
switchA#
Vlan : 1
-----
ARP Req Forwarded = 2
ARP Res Forwarded = 0
ARP Req Dropped   = 2
ARP Res Dropped   = 0
DHCP Drops        = 2
DHCP Permits      = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

## Configuring Device B

To enable DAI and configure Ethernet interface 1/4 on device B as trusted, follow these steps:



## Procedure

**Step 1** While logged into device B, verify the connection between device B and device A.

**Example:**

```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID         Local Intrfce  Hldtme  Capability  Platform      Port ID
switchA           Ethernet1/4    120     R S I       WS-C2960-24TC Ethernet2/3
switchB#
```

**Step 2** Enable DAI on VLAN 1, and verify the configuration.

**Example:**

```
switchB# config t
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----
Configuration      : Enabled
Operation State    : Active
switchB(config)#
```

**Step 3** Configure Ethernet interface 1/4 as trusted.

**Example:**

```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
Interface      Trust State    Rate (pps)    Burst Interval
-----
Ethernet1/4    Trusted        15            5
switchB#
```

**Step 4** Verify the list of DHCP snooping bindings.

**Example:**

```
switchB# show ip dhcp snooping binding
MacAddress      IpAddress      LeaseSec    Type          VLAN    Interface
-----
00:01:00:01:00:01  10.0.0.2      4995        dhcp-snooping  1       Ethernet1/4
switchB#
```

**Step 5** Check the statistics before and after DAI processes any packets.

**Example:**

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 0
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 0
SMAC Fails-ARP Req = 0
```

```

SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
switchB#

```

If Host 2 sends out an ARP request with the IP address 10.0.0.2 and the MAC address 0001.0001.0001, the packet is forwarded and the statistics are updated.

```

switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 1
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
switchB#

```

If Host 2 attempts to send an ARP request with the IP address 10.0.0.1, DAI drops the request and logs the following system message:

```

00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1. ([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jun 13 2008])

```

The statistics display as follows:

```

switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 1
ARP Res Forwarded = 0
ARP Req Dropped   = 1
ARP Res Dropped   = 0
DHCP Drops        = 1
DHCP Permits      = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
switchB#

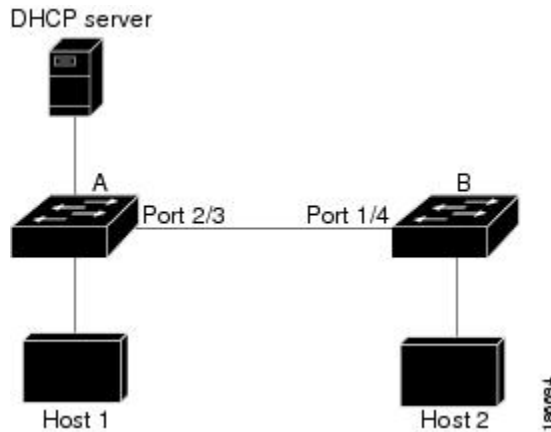
```

## Example 2 One Device Supports DAI

This procedure shows how to configure DAI when the second device involved in the network configuration does not support DAI or DHCP snooping.

Device B, shown in this figure does not support DAI or DHCP snooping; therefore, configuring Ethernet interface 2/3 on device A as trusted creates a security hole because both device A and Host 1 could be attacked by either device B or Host 2.

To prevent this possibility, you must configure Ethernet interface 2/3 on device A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of Host 2 is not static, which would make it impossible to accurately configure the ARP ACL on device A, you must separate device A from device B at Layer 3 and use a router to route packets between them.

**Figure 3: One Device Supporting DAI****Procedure**

- Step 1** Configure the access list to permit the IP address 10.0.0.1 and the MAC address 0001.0001.0001, and verify the configuration.

**Example:**

```
switchA# config t
switchA(config)# arp access-list H2
switchA(config-arp-acl)# permit ip host 10.0.0.1 mac host 0001.0001.0001
switchA(config-arp-acl)# exit
switchA(config)# show arp access-lists H2
ARP access list H2
10 permit ip host 1.1.1.1 mac host 0001.0001.0001
switchA(config)#
```

- Step 2** Apply the ACL to VLAN 1, and verify the configuration.

**Example:**

```
switchA(config)# ip arp inspection filter H2 vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 200
-----
Configuration      : Enabled
Operation State    : Active
ACL Match/Static   : H2 / No
```

- Step 3** Configure Ethernet interface 2/3 as untrusted, and verify the configuration.

**Note** By default, the interface is untrusted.

**Example:**

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# no ip arp inspection trust
switchA(config-if)# exit
switchA# show ip arp inspection interface ethernet 2/3
switchA#
```

The `show ip arp inspection interface` command has no output because the interface has the default configuration, which includes an untrusted state.

When Host 2 sends 5 ARP requests through Ethernet interface 2/3 on device A and a "get" is permitted by device A, the statistics are updated.

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 5
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

---

## Configuration Example for IP Source Guard

This example shows how to create a static IP source entry and then how to enable IP Source Guard on an interface.

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
 no shutdown
 ip verify source dhcp-snooping-vlan
```

## Configuration Examples for Password Encryption

The following example shows how to create a master key, enable the AES password encryption feature, and configure a type-6 encrypted password for a TACACS+ application:

```
key config-key ascii
 New Master Key:
 Retype Master Key:
configure terminal
feature password encryption aes
show encryption service stat
 Encryption service is enabled.
 Master Encryption Key is configured.
 Type-6 encryption is being used.
feature tacacs+
tacacs-server key Cisco123
show running-config tacacs+
 feature tacacs+
 logging level tacacs 5
 tacacs-server key 6
"JDYkqyIFWeBvzpljSfWmRZrmRSRE8syxKlOSjP9RCCkFinZbJI3GD5c6rckJR/Qju2PKLmOewbheAA=="
```

## Configuration Example for Keychain Management

This example shows how to configure a keychain named glbp keys. Each key text string is encrypted. Each key has longer accept lifetimes than send lifetimes, to help prevent lost communications by accidentally configuring a time in which there are no active keys.

```
key chain glbp-keys
  key 0
    key-string 7 zqdest
    accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
    send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
  key 1
    key-string 7 uaeqdyito
    accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
    send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
  key 2
    key-string 7 eekgsdyd
    accept-lifetime 00:00:00 Nov 12 2008 23:59:59 Mar 12 2009
    send-lifetime 00:00:00 Dec 12 2008 23:59:59 Feb 12 2009
```

## Configuration Example for Traffic Storm Control

The following example shows how to configure traffic storm control:

```
interface Ethernet1/1
  storm-control broadcast level 40
  storm-control multicast level 40
  storm-control unicast level 40
```

## Configuration Examples for Unicast RPF

The following example shows how to configure loose Unicast RPF for IPv4 packets:

```
interface Ethernet2/3
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via any
```

The following example shows how to configure strict Unicast RPF for IPv4 packets:

```
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

The following example shows how to configure loose Unicast RPF for IPv6 packets:

```
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

The following example shows how to configure strict Unicast RPF for IPv6 packets:

```
interface Ethernet2/4
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via rx
```

# Configuration Examples for CoPP

This section includes example CoPP configurations.

## CoPP Configuration Example

The following example shows how to configure CoPP using IP ACLs and MAC ACLs:

```

configure terminal
ip access-list copp-system-p-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-p-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-p-acl-arp
permit any any 0x0806

ip access-list copp-system-p-acl-tacas
permit udp any any eq 49

ip access-list copp-system-p-acl-gre
permit 47 any any

ip access-list copp-system-p-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-p-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-igmp
match access-group name copp-system-p-acl-msdp

class-map type control-plane match-any copp-system-p-class-important
match access-group name copp-system-p-acl-gre

class-map type control-plane match-any copp-system-p-class-normal
match access-group name copp-system-p-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option
match redirect arp-inspect
match redirect dhcp-snoop

policy-map type control-plane copp-system-p-policy

class copp-system-p-class-critical
police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform
transmit exceed transmit violate drop

class copp-system-p-class-important
police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform
transmit exceed transmit violate drop

class copp-system-p-class-normal
police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform
transmit exceed transmit violate drop

class class-default
police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform
transmit exceed transmit violate drop

control-plane
service-policy input copp-system-p-policy

```

## Changing or Reapplying the Default CoPP Policy Using the Setup Utility

The following example shows how to change or reapply the default CoPP policy using the setup utility.



### Note

Beginning with Cisco NX-OS Release 5.2, you can change or reapply the default CoPP policy using the **copp profile** command.

```
switch# setup

----- Basic System Configuration Dialog VDC: 1 -----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]: <CR>

Create another login account (yes/no) [n]: n

Configure read-only SNMP community string (yes/no) [n]: n

Configure read-write SNMP community string (yes/no) [n]: n

Enter the switch name : <CR>

Enable license grace period? (yes/no) [n]: n

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

Configure the default gateway? (yes/no) [y]: n

Configure advanced IP options? (yes/no) [n]: <CR>

Enable the telnet service? (yes/no) [n]: y

Enable the ssh service? (yes/no) [y]: <CR>

Type of ssh key you would like to generate (dsa/rsa) : <CR>

Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L3]: <CR>

Configure default switchport interface state (shut/noshut) [shut]: <CR>

Configure best practices CoPP profile (strict/moderate/lenient/skip) [strict]: strict

Configure CMP processor on current sup (slot 6)? (yes/no) [y]: n

Configure CMP processor on redundant sup (slot 5)? (yes/no) [y]: n

The following configuration will be applied:
password strength-check
no license grace-period
no telnet server enable
```

```

no system default switchport
system default switchport shutdown
policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#

```

## Preventing CoPP Overflow by Splitting ICMP Pings and ARP Requests

Some servers use ICMP pings and ARP requests to the default gateway to verify that the active NIC still has access to the aggregation switch. As a result, if the CoPP values are exceeded, CoPP starts dropping traffic for all networks. One malfunctioning server can send out thousands of ICMP pings and ARP requests, causing all servers in one aggregation block to lose their active NIC and start swapping NICs.

If your server is configured as such, you can minimize the CoPP overflow by splitting the ICMP pings and ARP requests based on subnets or groups of subnets. Then if a server malfunctions and overflows CoPP, the supervisor answers the ICMP pings and ARP requests only on some subnetworks.

The last entry in the class map or policy map should identify all of the ICMP pings and ARP requests in the networks that are not specified. If these counters increase, it means that a new network was added that was not specified in the existing ACLs for ICMP and ARP. In this case, you would need to update the ACLs related to ICMP and ARP.



**Note** Per the default CoPP, ICMP pings fall under `copp-system-p-class-monitoring`, and ARP requests fall under `copp-system-p-class-normal`.

The following example shows how to prevent CoPP overflow by splitting ICMP and ARP requests.

First, add the new ACLs that identify the networks you want to group together based on the findings of the investigations of the applications:

```

arp access-list copp-arp-1
statistics per-entry
10 permit ip 10.1.1.0 255.255.255.0 mac any
20 permit ip 10.1.2.0 255.255.255.0 mac any
30 permit ip 10.1.3.0 255.255.255.0 mac any
arp access-list copp-arp-2
statistics per-entry
10 permit ip 10.2.1.0 255.255.255.0 mac any
20 permit ip 10.2.2.0 255.255.255.0 mac any
30 permit ip 10.2.3.0 255.255.255.0 mac any
arp access-list copp-arp-3
statistics per-entry
10 permit ip 10.3.1.0 255.255.255.0 mac any
20 permit ip 10.3.2.0 255.255.255.0 mac any
30 permit ip 10.3.3.0 255.255.255.0 mac any
...
arp access-list copp-arp-10
10 permit ip any any mac any

ip access-list copp-icmp-1
statistics per-entry
10 permit icmp 10.2.1.0 255.255.255.0 any
20 permit icmp 10.2.2.0 255.255.255.0 any
30 permit icmp 10.2.3.0 255.255.255.0 any
ip access-list copp-icmp-2
statistics per-entry
10 permit icmp 10.3.1.0 255.255.255.0 any
10 permit icmp 10.3.2.0 255.255.255.0 any
10 permit icmp 10.3.3.0 255.255.255.0 any

```



```
ip access-list copp-icmp-3
statistics per-entry
10 permit icmp 10.4.1.0 255.255.255.0 any
10 permit icmp 10.4.2.0 255.255.255.0 any
10 permit icmp 10.4.3.0 255.255.255.0 any
...
ip access-list copp-icmp-10
10 permit icmp any any
```

Add these ACLs to the new class maps for CoPP:

```
class-map type control-plane match-any copp-cm-arp-1
 match access-group name copp-arp-1
class-map type control-plane match-any copp-cm-arp-2
 match access-group name copp-arp-2
class-map type control-plane match-any copp-cm-arp-3
 match access-group name copp-arp-3
...
class-map type control-plane match-any copp-cm-arp-10
 match access-group name copp-arp-10# class-map type control-plane match-any copp-cm-icmp-1
 match access-group name copp-icmp-1
class-map type control-plane match-any copp-cm-icmp-2
 match access-group name copp-icmp-2
class-map type control-plane match-any copp-cm-icmp-3
 match access-group name copp-icmp-3
...
class-map type control-plane match-any copp-cm-icmp-10
 match access-group name copp-icmp-10
```

Modify the CoPP policy map by adding new policies with the above created class maps:

```
policy-map type control-plane copp-system-p-policy
class copp-cm-icmp-1
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-2
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-3
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-4
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-10
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-1
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-2
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-3
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-4
 police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-10
 police cir X kbps bc X ms conform transmit violate drop
```

Delete ICMP and ARP from the existing class maps:

```
class-map type control-plane match-any copp-system-p-class-normal
no match protocol arp

class-map type control-plane match-any copp-system-p-class-monitoring
no match access-grp name copp-system-p-acl-icmp
```

## Configuration Examples for Rate Limits

The following example shows how to configure rate limits:

```
switch(config)# hardware rate-limiter layer-3 control 20000
```

```
switch(config)# hardware rate-limiter copy 40000
```

The following example shows how to configure rate limits globally on the device for packets that reach the supervisor module:

```
switch(config)# rate-limit cpu direction both pps 1000 action log
switch(config)# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 1000 outband pps global threshold 1000
```



## CHAPTER 5

# OTV Configuration Examples

---

Beginning with Cisco NX-OS Release 5.0(3), the Overlay Transport Virtualization (OTV) is available. This chapter provides examples on configuring OTV.

- [Configuration Examples for OTV, page 65](#)
- [Load Balancing Example, page 66](#)

## Configuration Examples for OTV

This example displays how to configure a basic OTV network that uses the configuration default values:

```
!Configure the physical interface that OTV uses to reach the
! DCI transport infrastructure
interface ethernet 2/1
 ip address 192.0.2.1/24
 ip igmp version 3
 no shutdown

!Configure the VLAN that will be extended on the overlay network
! and the site-vlan
vlan 2,5-10

! Configure OTV including the VLANs that will be extended.
feature otv
otv site-vlan 2
otv site-identifier 256
interface Overlay1
 otv control-group 239.1.1.1
 otv data-group 232.1.1.0/28
 otv join-interface ethernet 2/1
!Extend the configured VLAN
otv extend-vlan 5-10
 no shutdown
```

# Load Balancing Example

## Basic OTV Network

The following example displays how to configure load balancing on two edge devices in the same site:

```
Edge Device 1
interface ethernet 2/1
 ip address 192.0.2.1/24
 ip igmp version 3
 no shutdown

vlan 5-10

feature otv
otv site-identifier 256
interface overlay 1
 otv control-group 239.1.1.1
 otv data-group 239.1.1.0/29
 otv join-interface ethernet 2/1
 otv extend-vlan 5-10
 no shutdown
```

```
Edge Device 2
interface ethernet 1/1
 ip address 192.0.2.16/24
 ip igmp version 3
 no shutdown

vlan 5-10

feature otv
otv site-identifier 256
interface overlay 2
 otv control group 239.1.1.1
 otv data-group 239.1.1.0/29
 otv join-interface ethernet 1/1
 otv extend-vlan 5-10
 no shutdown
```