Digital Certificates/PKI for IPSec VPNs

This document provides information about using X.509 digital certificates issued by a Cisco IOS CA server to authenticate VPN tunnels between Cisco routers. It provides design considerations, step-by-step configuration instructions, and basic management options for VPN crypto devices using X.509 digital certificates. This document is written for Cisco system engineers and assumes that you have a working knowledge of Cisco IOS routers, as well as a basic understanding of IPSec, ISAKMP/IKE, and X.509 digital certificates.

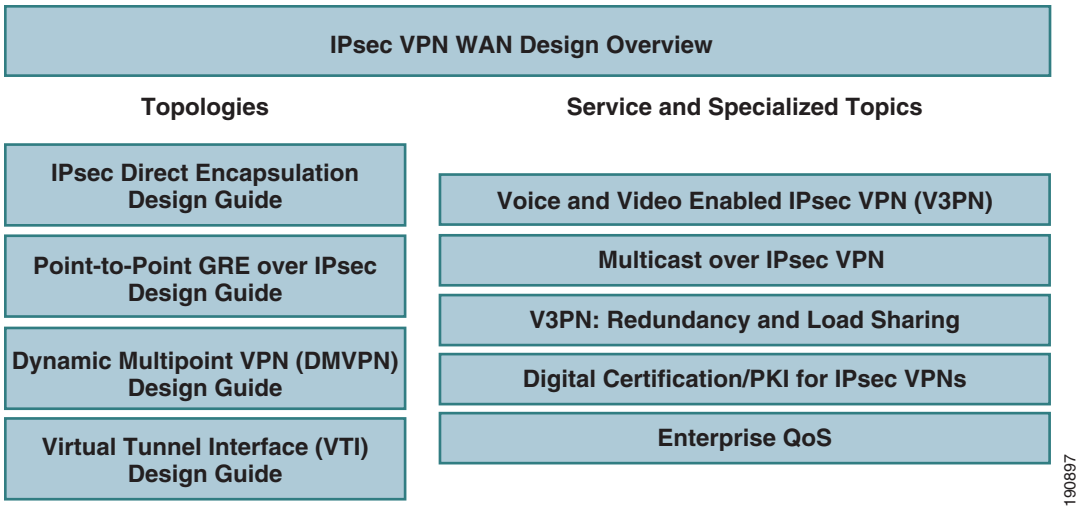
Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Design Guide Structure

This design overview is part of a series of design guides, each based on different technologies for the IPsec VPN WAN architecture. (See Figure 1.) Each technology uses IPsec as the underlying transport mechanism for each VPN.

Figure 1 IPsec VPN WAN Design Guides



Overview

A few basic mechanisms are available for authenticating VPN IPSec connections:

- Digital certificates
- Pre-shared static keys
- Pre-shared static keys with UserID Authentication (AAA with IPSec Aggressive mode authentication)

The best method to use in a specific network depends on the enterprise security policy. However, digital certificates provide many benefits compared to pre-shared keys, including the following:

- Centrally controlled on a digital certificate server, also known as a Certificate Authority (CA), or Public Key Infrastructure (PKI) server
- Built-in expiration dates
- Do not require IPSec Aggressive mode, which is required for the less secure pre-shared static keys with AAA
- Cannot be copied by an attacker, unlike other authentication measures, such as pre-shared keys.

A Cisco IOS CA server provides numerous benefits compared to a host-based CA, including the following:

- Runs as an integrated function within Cisco IOS software[1]
- Allows a router to be used as a one-armed server for higher server availability compared to traditional OS-based solutions
- Very reliable Simple Certificate Enrollment Protocol (SCEP) functions are provided by Cisco IOS software

1. The first Cisco IOS software image to support a CA server was 123-4.T. On this platform, both the Cisco IOS CA server and the headend and branch components of the VPN crypto routers were running the “cXXXX-advsecurityk9-mz.123-5.9.T” image.

- Less likely to be affected by common viruses, worms, and other forms of attack than traditional OS-based CAs
- Requires less overall system maintenance than a host-based server (fewer patches, service packs, and virus definition files)

Architectural Design Considerations

When using digital certificates for authenticating VPN tunnels, the main design considerations include the following:

- Network location—The CA server can located in a private network or on the public Internet.
  - Placing the CA server on a private network protects the CA server and lets it easily connect to internal corporate resources, such as an LDAP or Active Directory server. This is the recommended location because it provides a higher level of security.
  - Using a CA server on the public Internet lets you out source the CA to a third party or to make the CA publicly available.

  The appropriate location for your CA server depends on your security policies and access requirements. Table 1 lists the detailed advantages and disadvantages of each location.
- High availability—The CA server is a critical component of the IPSec VPN architecture and a clear plan to backup or replace the server is necessary. There are several choices to backup or replace the Cisco IOS CA. See the "Backing Up and Restoring the Cisco IOS CA Server" section on page 42, for information about the advantages and disadvantages of each method.
- Certificate revocation requirements—If certificate revocation is required, what is the maximum time that a revoked certificate is still allowed to connect? This depends on the Certification Revocation List (CRL) distribution time, the IPSec and ISAKMP SA lifetimes, and the Certification Distribution Point (CDP).
- Cryptographic key lengths for the X.509 Digital Certificates—The default, the allowed range, and the recommended length are as follows:
  - Default key length is 512 bytes
  - Supported key length is from 360 to 2048 bytes
  - Recommended key size is 1024 or higher
- The expiration time for the CRL lifetime—This is the interval after which the CRL on a VPN crypto-router expires and a new copy must be pulled from the Cisco IOS CA. The default, the allowed range, and the recommended length are as follows:
  - Default CRL lifetime is one week
  - Supported lifetime range is from 1 to 336 hours
  - Recommended CRL lifetime is 24 hours
- Cisco IOS CA server administration—Will the Cisco IOS CA server be administered manually by an administrator or will it automatically grant requests? Manually managing the CA server is more secure but requires more administration. Automatically granting requests (**auto grant**) requires less administration but is not as secure as manual administration. The appropriate option depends on enterprise security policies and the location of the CA server. See the "Automatically Re-enrolling Expired Certificates Before Expiration" section on page 37 for additional information.
- Need for IPSec Crypto Stateful Failover High Availability—Certificates for IPSec authentication are not supported for use with this feature.
- Availability of the K9 image—You will need a K9 image to do 3DES, shown in the examples in this document. To use AES for long keys, you need the K9 image for AES 128, 192, or 256 key lengths.

Table 1 Advantages and Disadvantages of CA Server Locations

Advantages	Disadvantages
CA Located in a Private Network	
• Supports cross-certification of other CA server hierarchies on the Enterprise Corporate Private Enterprise private network. • The CA server is protected from public access, and from intrusion or DoS attacks from the public Internet.	• Requires a slightly more complicated VPN router configuration. Because the CA server can not be reached on the public Internet, enrolling a new branch requires a VPN administrator to certificate enroll the VPN routers in one of the following ways: – Locally in the enterprise campus prior to shipping them to a remote location – Over an IPSec pre-shared tunnel connection. – Interactively through cut-and-paste certificate enrollment over a telnet/ssh session to a remote VPN router. • Because the CA server cannot be reached from the public Internet it cannot be used for other Cisco-specific applications that have public X.509 certificates requirements.
CA Located in a Public Network	
• Provides a CA server that can be used for IPSec tunnels or other Cisco-specific applications that have public X.509 certificates requirements. • Provides the simplest enrollment for the VPN endpoint routers. • Provides for cross-certification of other CA servers hierarchies on the public Internet.	• Because the CA server is available to the public it is a possible target for intrusion or DoS attacks. Precautions must be taken to protect the server.

Configuring the Cisco IOS CA Server

This section shows an example of a typical configuration of a Cisco IOS CA server. Several VPN endpoints (routers) can enroll with the CA server. In this example, the following files are saved to the NVRAM on the Cisco IOS CA device:

- A copy of the CA certificates
- The public-private key pair
- An information file for each certificate that is issued

You can also choose to store these items in flash, disk/slot, or even to a host-based server on a different system using TFTP.

Note In this document, the certificate logs generated on the Cisco IOS CA server were stored on the NVRAM in a lab environment. In an actual production environment the location of the storage should be a removable media card, such as a flash or compact flash card, referred to as slot/disk in the Cisco IOS software CLI).

With Cisco IOS software Version 12.4(T) a "split database" feature will be available for the Cisco IOS CA server. This will allow mission-critical files to be stored on the Cisco IOS CA server filesystem, while log files, which are not critical to server operation, can be stored externally on a different server. This new feature overcomes most of the disadvantages of off-system storage and gives the CA administrator the best of both worlds. The examples in this document do not illustrate the split database feature because it is not yet available at the time that this document is being written.

Caution Before performing CA server configuration, determine the values you want to use for the various PKI system settings, such as certificate lifetime, CRL lifetime, and the CDP. Once these settings are entered for a Cisco IOS CA server and the certificates have been generated, to make any further changes you must reconfigure the Cisco IOS CA server and re-enroll all of the branches.

Before starting, note that only the default files are stored in NVRAM. To display the contents of the NVRAM and verify that these files are present, enter the following command:

```
dir nvram:
! Directory of nvram:/
!
!   52  -rw-        2151                    <no date>  startup-config
!   53  ----          24                    <no date>  private-config
!    1  -rw-           0                    <no date>  ifIndex-table
!    2  ----          12                    <no date>  persistent-data
!
! 57336 bytes total (53061 bytes free)
```

To configure a Cisco IOS CA, perform the following steps:

Step 1 To enable the HTTP server daemon, enter the following commands:

```
conf t
ip http server
```

The HTTP daemon is used by Simple Certificate Enrollment Protocol (SCEP) for enrollment and CRL distribution.

Step 2 To configure the Network Time Protocol (NTP) to synchronize the time with the stratum clock, enter the following commands:

```
clock timezone EST -5
clock summer-time EDT recurring
ntp peer 172.26.176.10
```

Step 3 To create a labeled public and private key pair, enter the following command:

```
crypto key generate rsa general-keys label ese-ios-ca modulus 1024 exportable
```

In this example:

- **label** is the keyword identifying the key-label named **ese-ios-ca**
- **modulus** is the keyword specifying that the key length is **1024**
- **exportable** is required to back-up the key pairs to a storage device

The command syntax is as follows:

crypto key generate rsa general-keys label *key-label* **exportable**

The **exportable** option is required to backup the key pair, as shown in Step 4.

Note You must use the same name for the key pair (*key-label*) that you plan to use for the certificate server *cs-label* in the **crypto pki server** command, shown in Step 6.

When the key pair is created, messages such as the following are displayed:

```
!The name for the keys will be: ese-ios-ca
!% The key modulus size is 1024 bits
!% Generating 1024 bit RSA keys ...[OK]
```

You must wait until the certificate server has been generated before entering the **no shut** command.

Note You can use the **crypto ca export pkcs12** command to export a pkcs12 file that contains the server certificate as well as the private key.

Step 4 To export your key pairs to a storage device, enter the following command:

crypto key export rsa *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

For example:

crypto key export rsa ese-ios-ca pem url nvram: 3des cisco123

In this example:

- **ese-ios-ca** is the name of the key pair.
- **url nvram** points to the NVRAM
- **cisco123** is the passphrase

Note It is very important to remember the passphrase chosen during the key generation process. This passphrase will be *required* to re-import these keys to a new Cisco IOS CA, in the event of a CA system failure.

When you enter this command correctly, the following messages are displayed:

```
!% Key name: ese-ios-ca
!   Usage: General Purpose Key
!Exporting public key...
!Destination filename [ese-ios-ca.pub]?
<return>

!Writing file to nvram:ese-ios-ca.pub
!
!Exporting private key...
!Destination filename [ese-ios-ca.prv]?
<return>

!Writing file to nvram:ese-ios-ca.prv
```

Step 5 (Optional) To verify that the necessary files have been created, view the contents of NVRAM by entering the following command:

```
dir nvram:
! Directory of nvram:/
!
!   50  -rw-        2420                    <no date>  startup-config
!   51  ----        1924                    <no date>  private-config
!    1  -rw-           0                    <no date>  ifIndex-table
!    2  ----          12                    <no date>  persistent-data
!    3  -rw-         272                    <no date>  ese-ios-ca.pub
!    4  -rw-         963                    <no date>  ese-ios-ca.prv
!
! 57336 bytes total (48844 bytes free)
```

In this example two new files are highlighted (ese-ios-ca.pub and ese-ios-ca.prv) which have been added to NVRAM. These files contain the public (.prv) and private (.prv) keys for the Cisco IOS CA. These files are used in the backup procedure described in the "Backing Up and Restoring the Cisco IOS CA Server" section on page 42.

The following steps determine the configuration for the certificates that are issued, set important fields in the certificate, and enable the certificate.

Step 6 To create the PKI server, enter the following command:

crypto pki server *cs-label*

In this example, the value for *cs-label* would be:

```
crypto pki server ese-ios-ca
```

Step 7 To set the level of database information to be written (to help limit NVRAM size), enter the following command:

database level {**minimal** | **names** | **complete**}

This command controls the type of data that is stored in the certificate enrollment database. The options are as follows:

- **minimal**—Enough information is stored to continue issuing new certificates without conflict. This is the default.
- **names**—In addition to the information given by the minimal option, this includes the serial number and subject name of each certificate.
- **complete**—In addition to the information given by the minimal and names options, each issued certificate is written to the database.

Step 8 To specify the location to write the certificate server data entries, enter the following command:

database url *root-url*

Where *root-url* is the location for the database entries.

In this example, use the **names** option, as in the following example:

```
database level names
```

If this command is not specified, database entries are written to NVRAM.

The following are examples:

```
database url tftp://mytftp
database url nvram
```

Step 9 To set the issuer name, as specified by the CN field (issuer-name cn=ca-label), enter the following command:

```
issuer-name CN = ese-ios-ca, OU = ESE, O = Cisco Systems Inc, L = Raleigh, ST = NC, C =
US, EA = ese-vpn-team
```

In this example, the CN field identifies the the Cisco IOS CA instance.

Note At the very least, you must specify the value of the CN field. The other parameters are optional.

Step 10 To set the CRL lifetime in hours, enter the following command:

```
lifetime crl 24
```

This step defines the lifetime of the CRL used by the certificate server for 24 hours, which is a generally recommended value.

The default is 168 hours (one week). The maximum value is 336 hours (two weeks). The actual value you should use depends on your enterprise security policy.

Step 11 To set the lifetime of certificates issued by this CA in days, enter the following command:

```
lifetime certificate days
```

The generally recommended certificate lifetime is 750 days (two years), but the actual value you should use depends on your enterprise security policy. This example sets the lifetime for 254 days:

```
lifetime certificate 254
```

Step 12 To set the lifetime of the CA signing certificate in days, enter the following command:

```
lifetime ca-certificate days
```

The command syntax is as follows:

lifetime {**ca-certificate** | **certificate**} *time*

The valid values range is from 1 to 1825 days (five years). The following example sets the lifetime for 508 days.

```
lifetime ca-certificate 508
```

The default certificate lifetime is 365 days (one year). The default CA certificate lifetime is three years. The generally recommended CA certificate lifetime is between 1095 and 1825 days (three to five years).

Note A certificate is only valid as long the certificate itself and the certificate of the issuing CA remain valid.

Step 13 (Optional) To automatically grant all requests for certificate enrollment to this CA, enter the following command:

```
grant auto
yes
```

Whether you enable automatic enrollment or re-enrollment in a production environment depends on your enterprise security policy and CA administrative restrictions. Manually administering certificate enrollment and re-enrollment in a large certificate deployment can be laborious unless you use the **grant auto** command. For further information, see the "Enrollment with a Cisco IOS Software CA Over SCEP" section on page 13.

The command syntax is as follows:

```
grant [auto | none ]
```

Step 14 After completing your certificate server configuration, enter the **no shutdown** command for the PKI server subsystem, as in the following example:

```
no shutdown
      ! % Once you start the server, you can no longer change some of
      ! % the configuration.
      ! Are you sure you want to do this? [yes/no]:
    yes
      ! % Certificate Server enabled.
```

As shown in this example, type **yes** in response to the system prompt. A few seconds normally elapse between your response and the enable message.

Step 15 To confirm that the certificate was created, enter the following commands:

```
end
show crypto pki server
```

The first command displays the enable prompt. The second command displays the current PKI server state, as in the following example:

```
! Certificate Server status: enabled, configured
  !    Granting mode is: manual
  !    Last certificate issued serial number: 0x1
  !    CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
  !    CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
  !    Current storage dir: nvram:
  !    Database Level: Names - subject name data written as <serialnum>.cnm
```

Step 16 To confirm that the CA was created, enter the following command:

```
show crypto ca certificate
```

```
The system displays the following output:
! CA Certificate
  !  Status: Available
  !  Certificate Serial Number: 01
  !  Certificate Usage: Signature
  !  Issuer:
  !    cn=ese-ios-ca
  !    ou=ESE
  !    o=Cisco Systems Inc
  !    l=Raleigh
  !    st=NC
  !  Subject:
  !    cn=ese-ios-ca
  !    ou=ESE
  !    o=Cisco Systems Inc
  !    l=Raleigh
  !    st=NC
  !  Validity Date:
  !    start date: 09:58:20 EST Jan 30 2004
  !    end   date: 10:58:20 EDT Jun 21 2005
  !  Associated Trustpoints: ese-ios-ca
```

Step 17 To save the certificate, enter *one* of the following commands:

```
copy run start
```

or

```
wr mem
```

Note This step is very important.

The following is an example of the **copy run start** command:

```
copy run start
  ! Destination filename [startup-config]?
<return>
  ! Building configuration...
  ! [OK]
```

Step 18 (Optional) To view the results, enter the following command:

```
dir nvram
```

The system displays the following information:

```
! Directory of nvram:/
  !
  !   50  -rw-        2148                    <no date>  startup-config
  !   51  ----        1924                    <no date>  private-config
  !    1  -rw-           0                    <no date>  ifIndex-table
  !    2  ----          12                    <no date>  persistent-data
  !    3  -rw-         272                    <no date>  ese-ios-ca.pub
  !    4  -rw-         963                    <no date>  ese-ios-ca.prv
  !    5  -rw-         112                    <no date>  1.cnm
  !    6  -rw-          32                    <no date>  ese-ios-ca.ser
  !    7  -rw-         300                    <no date>  ese-ios-ca.crl
  !    8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
  !
  ! 57336 bytes total (43574 bytes free)
```

The sample output shows that the following files have have been created:

- 1.cnm, the name of certificate file, containing the certificate serial number “1” (hexadecimal).
- ee-ios-ca.ser—the CA counter file
- ese-ios-ca.crl—the current version of the CRL for distribution to requesters
- ese-ios-ca#6001CA.cer—the CA signing certificate

The NVRAM contains one or more files with names similar to “1.cmn” for each issued certificate, with 1.cmn being the first issued certificate. You can view the information for each certificate, as in the following example:

```
more nvram:1.cnm
  ! subjectname_str = cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
  ! expiration = 10:58:20 EDT Jun 21 2005
```

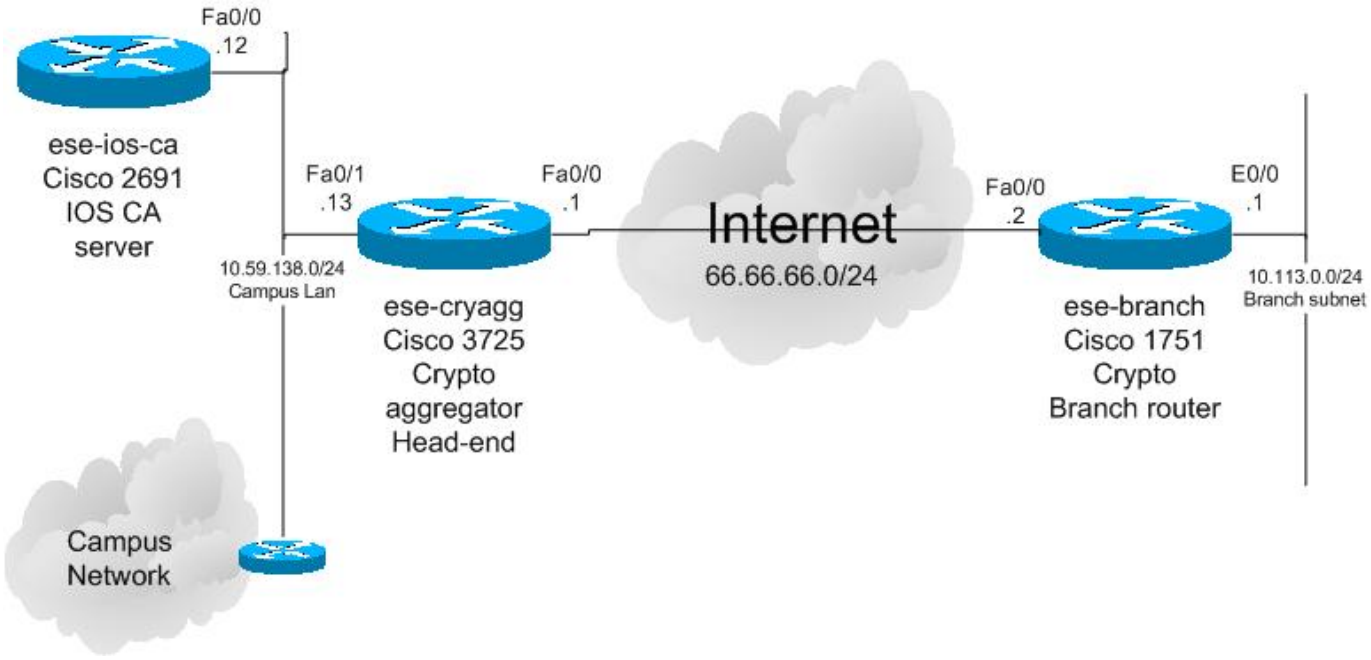
This example logs database level names. The file lists the subjectname string, in which the CN should be the device name. The filename contains the serial number of the certificate (1.cnm is serial number 1), and it lists that certificate expiration date.

See the “Viewing Issued Certificates” section on page 54 for additional commands to display information in the NVRAM file.

Enrollment with a Cisco IOS Software CA Over SCEP

In this example, the Cisco IOS CA is located in a private subnet in the enterprise campus network and is not directly accessible to the Internet (see Figure 2). Accessibility from the Internet slightly changes certificate enrollment configuration on both the crypto headend and the crypto branches.

Figure 2 Headend Location in a Private Network



In this example, both the crypto headend router and the crypto branch router are configured with a crypto IPSec tunnel using pre-shared keys as a prep-tunnel for the certificate enrollment. To enroll a certificate, remove the pre-shared key from the headend and use the certificate for IPSec authentication of the IPSec tunnel.

This example illustrates a hub-and-spoke VPN architecture. All communication from a branch goes to the VPN crypto headend—even traffic destined for another VPN branch. The branch router can only reach the CA server over an IPSec tunnel. Using a prep-tunnel gives the branch a way of reaching the internal CA server and enrolling. After enrollment is complete, the pre-shared key on the headend can be deleted from the VPN router or from the crypto headend system.

The crypto headend router is connected directly through the network to the CA server by a LAN port for straightforward SCEP certificate enrollment. Because the headend router is directly connected to the CA server, it is not necessary to source the enrollment request. To verify that the prep-tunnel is working with the pre-shared keys, enter the following command:

```
show crypto isa sa detail
  ! Codes: C - IKE configuration mode, D - Dead Peer Detection
  !        K - Keepalives, N - NAT-traversal
  !        X - IKE Extended Authentication
  !        psk - Preshared key, rsig - RSA signature
  !        renc - RSA encryption
  !
  ! C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
  ! 1     66.66.66.2      66.66.66.1               3des sha  psk  2  01:54:30 D
  !       Connection-id:Engine-id =  1:1(software)
```

The term psk in the sample output stands for pre-shared key.

IPSec Headend Hub-and-Spoke Configuration Using dmaps (DPD/RRI)

The following example illustrates hub-and-spoke configuration on the crypto headend with dmaps, which use Dead Peer Detection/Reverse Route Injection (DPD/RRI).

```
!
crypto isakmp policy 10
  encr 3des
  ! Note the default authentication is Digital Certificates
  ! by not listing a authentication we are saying to use certificates (rsig)
  group 2
!
!The following isakmp policy is for the pre-shared prep tunnel
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key bigsecret address 66.66.66.2
crypto isakmp keepalive 10
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
!
interface FastEthernet0/0
 description OUTSIDE (toward Internet)
 ip address 66.66.66.1 255.255.255.0
 crypto map dynamic-map
!
```

Branch End Hub-and-Spoke Configuration

The following example illustrates hub-and-spoke configuration on the branch end using static crypto peer DPD to the headend (IPSec Direct Encapsulation).

```
!
crypto isakmp policy 10
  encr 3des
  ! Note the default authentication is Digital Certificates
  ! by not listing a authentication we are saying to use certificates (rsig)
  group 2
!
!The following isakmp policy is for the pre-shared prep tunnel
crypto isakmp policy 20
 encr 3des
```

```
 authentication pre-share
 group 2
!
crypto isakmp key bigsecret address 66.66.66.1
crypto isakmp keepalive 10
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto map test 10 ipsec-isakmp
 description Calls the dynamic map on the crypto HE box(es)
 set peer 66.66.66.1
 set transform-set vpn-test
 match address CryptoMapACL
 qos pre-classify
!
interface FastEthernet0/0
 description OUTSIDE (toward Internet)
 ip address 66.66.66.2 255.255.255.0
 crypto map test
!
!
ip access-list extended CryptoMapACL
 permit ip 10.113.0.0 0.0.0.255 10.0.0.0 0.255.255.255
 deny   ip any any
 remark This ACL is a filter of which traffic is for the crypto ipsec tunnel
!
```

Enrolling a VPN Headend Router with the Cisco IOS CA Using SCEP

To enroll the VPN headend router, complete the following steps:

Step 1 To verify network reachability from this router to the CA server, enter the following command:

```
ping 10.59.138.12
  !
  ! Type escape sequence to abort.
  ! Sending 5, 100-byte ICMP Echos to 10.59.138.12, timeout is 2 seconds:
  ! !!!!!
  ! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

If you cannot reach the network, there is a network or routing problem that needs to be resolved before proceeding. For example, the following command pings for a CA server with the address of 10.59.138.12.

Step 2 To set the time and hostname, enter the following commands:

```
terminal monitor
conf t
ip hostname ese-cryagg
clock timezone EST -5
clock summer-time EDT recurring
ip domain name ese.cisco.com
ip host ese-ios-ca 10.59.138.12
ntp server 172.26.176.10
```

Set the router clock either manually with the **set clock** command, or with the **ntp** command using a time server. Certificates have built-in expiration times that are checked against the system times before a certificate can be used.

Assigning a hostname identifies the host for subsequent enrollment commands, additional configuration, and provides flexibility in case the IP address of the CA server changes.. The following is an example:

Step 3 To create a public/private key pair, enter the following command:

crypto key generate rsa general-keys modulus 1024

```
! The name for the keys will be: ese-cryagg.ese.cisco.com
!
! % The key modulus size is 1024 bits
! % Generating 1024 bit RSA keys ...[OK]
```

Unlike creating a key pair on the Cisco IOS CA, keys for the headend router do not need to be labeled. The **crypto key generate** command can take time to complete.

Step 4 Create and configure a trustpoint to the Cisco IOS CA server.

a. To create a trustpoint for the CA, enter the following command:

```
crypto ca trustpoint ese-ios-ca
```

If you skip the enrollment mode, the router automatically determines whether or not the mode is **ra** after authentication. The mode is stored in the router configuration and is preserved through reboots.

b. (Optional) To choose an enrollment mode, enter the following command:

```
enrollment mode ra
```

RA mode is the only mode currently available and is the default.

c. To enter the SCEP enrollment path, enter the following command:

```
enrollment url http://ese-ios-ca:80
```

Note Do not add a trailing "/" to the URL as this will cause authentication to fail.

d. To set enforced CRL checking, enter the following command:

```
revocation-check crl
```

In a hub-and-spoke topology, the crypto headend should always check the CRL; in this topology it is optional for the crypto branch routers to check the CRL. In a Full/Partial mesh all crypto routers should check the CRL.

e. To set automatic enrollment, enter the following command:

```
auto-enroll 70
exit
```

You may also execute this command after you have enrolled the router.

Step 5 To authenticate to the CA, enter the following command:

```
crypto ca authenticate ese-ios-ca
      ! Certificate has the following attributes:
      ! Fingerprint: 9D8D787D 574D2955 CA666B2B 22F3C31A
      ! % Do you accept this certificate? [yes/no]:
yes
      ! Trustpoint CA certificate accepted.
```

Type **yes** when prompted, as shown in this example.

Step 6 To request enrollment to the CA, enter the following command and respond to the system prompts:

```
crypto ca enroll ese-ios-ca
! %
! % Start certificate enrollment ..
! % 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:
whatever
! Re-enter password:
whatever
!
! % The fully-qualified domain name in the certificate will be: ese-cryagg.ese.cisco.com
! % The subject name in the certificate will be: ese-cryagg.ese.cisco.com
! % Include the router serial number in the subject name? [yes/no]:
no
!% Include an IP address in the subject name? [no]:
no
! Request certificate from CA? [yes/no]:
yes
! % Certificate request sent to Certificate Authority
! % The certificate request fingerprint will be displayed.
! % The 'show crypto ca certificate' command will also show the fingerprint.
```

After completing this step successfully, the CA issues the certificate.

The recommend configuration is to not include either the router serial or IP address as it makes certificate management more complex and more likely to require corrections to the certificate if the router or the IP address change. Note that the IP address of the outside interface changes frequently when a branch router is in a broadband deployment or where the Public Internet IP address is assigned by DHCP.

Once the enrollment is approved by the CA administrator or the request fails or times out, a **conf t** prompt is issued. See the "Approving an Enrollment for the VPN Headend Router on the Cisco IOS CA" section on page 19 for more information about how the certificate administrator approves an enrollment.

Step 7 To save the certificate on the router, enter the following commands:

```
end
copy run start
  ! Destination filename [startup-config]?
<return>
  ! Building configuration...
  ! [OK]
```

Note It is very important to execute this command on the router that just requested enrollment.

Step 8 To verify that there are two certificates (one for the CA and one for the router), enter the following command:

```
show crypto ca certificates
  ! Certificate
  !   Status: Available
  !   Certificate Serial Number: 02
  !   Certificate Usage: General Purpose
  !   Issuer:
  !     cn=ese-ios-ca
  !     ou=ESE
  !     o=Cisco Systems Inc
  !     l=Raleigh
  !     st=NC
  !   Subject:
  !     Name: ese-cryagg.ese.cisco.com
  !     hostname=ese-cryagg.ese.cisco.com
  !   Validity Date:
  !     start date: 14:40:01 EST Jan 30 2004
  !     end   date: 15:40:01 EDT Oct 10 2004
  !     renew date: 10:52:01 EDT Jul 26 2004
  !   Associated Trustpoints: ese-ios-ca
  !
  !
  ! CA Certificate
  !   Status: Available
  !   Certificate Serial Number: 01
  !   Certificate Usage: Signature
  !   Issuer:
  !     cn=ese-ios-ca
  !     ou=ESE
  !      o=Cisco Systems Inc
  !     l=Raleigh
  !     st=NC
  !   Subject:
  !     cn=ese-ios-ca
  !     ou=ESE
  !     o=Cisco Systems Inc
  !     l=Raleigh
  !     st=NC
```

```
!   Validity Date:
!     start date: 09:58:20 EST Jan 30 2004
!     end   date: 10:58:20 EDT Jun 21 2005
!   Associated Trustpoints: ese-ios-ca
```

Step 9 To verify that the certificates are stored in NVRAM of the router, enter the following command:

```
dir nvram:
  ! Directory of nvram:/
  !
  !    50  -rw-        2739                    <no date>  startup-config
  !    51  ----        1934                    <no date>  private-config
  !     1  -rw-           0                    <no date>  ifIndex-table
  !     2  -rw-         566                    <no date>  ese-ios-ca#6102.cer
  !     3  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
  !
      ! 57336 bytes total (49539 bytes free)
```

In this example, the certificates are identified by the .cer extension. The numerical portion of the certificate name can be translated as follows:

- "61" means the item is a certificate
- "01" and "02" are the certificate serial numbers in hexadecimal
- "CA" is the CA server signature

Approving an Enrollment for the VPN Headend Router on the Cisco IOS CA

The following example shows the events that occur on the Cisco IOS CA server when manually approving an enrollment request.

Note This process is only required if **grant auto** was not set on the Cisco IOS CA server.

```
crypto pki server ese-ios-ca info requests
! Enrollment Request Database:
! ReqID  State      Fingerprint                      SubjectName
! --------------------------------------------------------------------
! 1      pending    93453F440CEA2DB76BB826DDC58C8949 hostname=ese-cryagg.ese.cisco.com
!
crypto pki server ese-ios-ca grant ?
!   <1-999>  Transaction ID
!   all      all pending requests
!
crypto pki server ese-ios-ca grant 1
crypto pki server ese-ios-ca info requests
! Enrollment Request Database:
! ReqID  State      Fingerprint                      SubjectName
! --------------------------------------------------------------------
! 1      granted    93453F440CEA2DB76BB826DDC58C8949 hostname=ese-cryagg.ese.cisco.com
!
dir nvram:
! Directory of nvram:/
!
!    50  -rw-        2570                    <no date>  startup-config
!    51  ----        1924                    <no date>  private-config
!     1  -rw-           0                    <no date>  ifIndex-table
```

```
!      2  ----          12                    <no date>  persistent-data
!      3  -rw-         272                    <no date>  ese-ios-ca.pub
!      4  -rw-         963                    <no date>  ese-ios-ca.prv
!      5  -rw-         112                    <no date>  1.cnm
!      6  -rw-          32                    <no date>  ese-ios-ca.ser
!      7  -rw-         300                    <no date>  ese-ios-ca.crl
!      8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
!      9  -rw-          89                    <no date>  2.cnm
!
! 57336 bytes total (43574 bytes free)
more nvram:2.cnm
! subjectname_str = hostname=ese-cryagg.ese.cisco.com
! expiration = 15:40:01 EDT Oct 10 2004
```

Enrolling a Branch Router with a Cisco IOS CA Using SCEP

In this example, the Cisco IOS CA is located in a private subnet in the enterprise campus network and cannot be accessed directly from the Internet. The process and commands for a VPN branch enrollment are almost identical to the headend with the following two exceptions:

- Branch communication with the Cisco IOS CA server must go through the prep-tunnel to reach the CA server. For this reason, the enrollment needs to be sourced from the LAN interface so that the authentication and enrollment traffic matches the IPSec crypto access control list and is put into the prep-tunnel.
- The branches do not need to check the CRL in a hub-and-spoke topology, so the CRL can be either defined as optional or omitted.

Note Branches need the pre-shared prep-tunnel only for initial enrollment. To re-enroll before it expires use the **auto-enroll** command over an existing IPSec tunnel that was authenticated by the previous certificate. See the "Automatically Re-enrolling Expired Certificates Before Expiration" section on page 37 for more information.

To enroll over SCEP to a Cisco IOS CA branch server, perform the following steps:

Step 1 To verify network reachability from this router to the CA server, enter the following command:

```
ping ip 10.59.138.12 source 10.113.0.1 repeat 15
  !
  ! Type escape sequence to abort.
  ! Sending 15, 100-byte ICMP Echos to 10.59.138.12, timeout is 2 seconds:
  ! Packet sent with a source address of 10.113.0.1
  ! ....!!!!!!!!!!!!
  ! Success rate is 93 percent (14/15), round-trip min/avg/max = 4/5/8 ms
```

This example pings for a CA server with the address of 10.59.138.12 from the LAN side of the server. It is not unusual for the first few pings to fail. If you cannot reach the network, there is a network or routing problem that needs to be resolved before proceeding.

Step 2 To set the time and the hostname, enter the following commands:

```
terminal monitor
conf t
    ip hostname ese-branch
    clock timezone EST -5
    clock summer-time EDT recurring
    ip domain name ese.cisco.com
```

```
ip host ese-ios-ca 10.59.138.12
ntp server 172.26.176.10
```

Note You *must* set the router clock either manually with the **set clock** command, or by using the **ntp** command to set the time using a time server. Certificates have built-in expiration times that are checked against the system times before a certificate can be used.

Setting the hostname makes configuration easier and provides flexibility in case the IP address of the CA server changes.

Step 3 To create a public/private key pair, enter the following command:

```
crypto key generate rsa general-keys modulus 1024
    !  The name for the keys will be: ese-branch.ese.cisco.com
    !
    ! % The key modulus size is 1024 bits
    ! % Generating 1024 bit RSA keys ...[OK]
```

A 1024-byte key is used in all the examples in this document.

Note Be patient because it is normal for this command to take some time to complete.

Unlike creating a key pair on the Cisco IOS CA, you do not need to make these keys exportable or label the key pair. By default, Cisco IOS uses the router hostname for the CN field in the DN string.

Step 4 Create and configure a trustpoint to the Cisco IOS CA server.

a. To create a trustpoint for the CA, enter the following command:

```
crypto ca trustpoint ese-ios-ca
```

If you skip the enrollment mode, the router automatically determines whether or not the mode is **ra** after authentication. The mode is stored in the router configuration and is preserved through reboots.

b. (Optional) To choose an enrollment mode, enter the following command:

```
enrollment mode ra
```

c. To enter the SCEP enrollment path, enter the following command:

```
enrollment url http://ese-ios-ca:80
```

Note Do not add a trailing "/" to the URL as this will cause authentication to fail.

d. To set enforced CRL checking, enter the following command:

```
revocation-check crl
```

Crypto headends always check the CRL in a "hub-and-spoke" topology. Crypto headends and branches must also check the CRL in a full-mesh topology. It is optional for crypto branches to check the CRL.

e. If the CA server is located in the private enterprise subnet, source your request from the LAN interface of the branch router.

```
source interface Ethernet0/0
```

In this example the LAN interface is Ethernet0/0.

f. To set automatic enrollment, enter the following command:

```
auto-enroll 70
exit
```

You may also execute this command after you have enrolled the router.

Step 5 To authenticate to the CA, enter the following command and respond to the system prompt:

```
crypto ca authenticate ese-ios-ca
! Certificate has the following attributes:
! Fingerprint: 9D8D787D 574D2955 CA666B2B 22F3C31A
! % Do you accept this certificate? [yes/no]:
yes
! Trustpoint CA certificate accepted.
```

Step 6 To request enrollment to the CA, enter the following command and respond to the system prompts:

```
crypto ca enroll ese-ios-ca
! %
! % Start certificate enrollment ..
! % 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:
whatever
! Re-enter password:
whatever
!
! % The fully-qualified domain name in the certificate will be: ese-cryagg.ese.cisco.com
! % The subject name in the certificate will be: ese-cryagg.ese.cisco.com
! % Include the router serial number in the subject name? [yes/no]:
no
! % Include an IP address in the subject name? [no]:
no
! Request certificate from CA? [yes/no]:
yes
! % Certificate request sent to Certificate Authority
! % The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
```

When this step completes successfully, the CA issues the certificate.

The recommend configuration is to not include either the router serial or IP address as it makes certificate management more complex. Corrections to the certificate will be required if the router or the IP address of the router changes. Note that the IP address of the outside interface changes frequently in a broadband type deployment for a branch router, or when DHCP is used to assign the public Internet IP address.

Once the enrollment is approved by the CA administrator or the request fails or times out, a **conf t** prompt is issued. See the "Approving an Enrollment for a Branch Router with a Cisco IOS CA" section on page 24 for more information about how the certificate administrator approves an enrollment.

Step 7 To save your certificate on the router, enter the following commands:

```
end
copy run start
  ! Destination filename [startup-config]?
<return>
  ! Building configuration...
  ! [OK]
```

Note It is very important to execute this command on the router that just requested enrollment.

Step 8 To verify that there are two certificates (one for the CA and one for the router), enter the following command:

```
show crypto ca certificates
  ! Certificate
  !  Status: Available
  !  Certificate Serial Number: 03
  !  Certificate Usage: General Purpose
  !  Issuer:
  !   cn=ese-ios-ca
  !    ou=ESE
  !    o=Cisco Systems Inc
  !    l=Raleigh
  !    st=NC
  !  Subject:
  !    Name: ese-branch.ese.cisco.com
  !    hostname=ese-branch.ese.cisco.com
  !  Validity Date:
  !    start date: 16:10:10 EST Jan 30 2004
  !    end   date: 17:10:10 EDT Oct 10 2004
  !    renew date: 12:22:10 EDT Jul 26 2004
  !  Associated Trustpoints: ese-ios-ca
  !
  ! CA Certificate
  !  Status: Available
  !  Certificate Serial Number: 01
  !  Certificate Usage: Signature
  !  Issuer:
  !    cn=ese-ios-ca
  !    ou=ESE
  !    o=Cisco Systems Inc
  !    l=Raleigh
  !    st=NC
  !  Subject:
  !    cn=ese-ios-ca
  !    ou=ESE
  !    o=Cisco Systems Inc
  !    l=Raleigh
  !    st=NC
  !  Validity Date:
  !    start date: 09:58:20 EST Jan 30 2004
  !    end   date: 10:58:20 EDT Jun 21 2005
  !  Associated Trustpoints: ese-ios-ca
```

Step 9 To verify that the certificates are stored in NVRAM, enter the following command:

```
dir nvram:
  ! Directory of nvram:/
  !
  !   23  -rw-        2878                    <no date>  startup-config
  !   24  ----        1962                    <no date>  private-config
  !    1  -rw-           0                    <no date>  ifIndex-table
  !    2  -rw-         566                    <no date>  ese-ios-ca#6103.cer
  !    3  ----          12                    <no date>  persistent-data
  !    4  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
  !
  ! 29688 bytes total (20700 bytes free)
```

In this example, the certificates are identified by the .cer extension. The numerical portion of the certificate name can be translated as follows:

- “61” means the item is a certificate
- “01” and “03” are the certificate serial numbers in HEX
- “CA” is the CA server signature

Approving an Enrollment for a Branch Router with a Cisco IOS CA

The following example shows the events that occur on the Cisco IOS CA server when manually approving an enrollment request.

Note This process is only required if **grant auto** was not set in the Cisco IOS CA server.

```
crypto pki server ese-ios-ca info requests
! Enrollment Request Database:
! ReqID  State      Fingerprint                      SubjectName
! --------------------------------------------------------------------
!  2      pending    0784BC89DE717A105ABD9B2260FE5F53 hostname=ese-branch.ese.cisco.com
crypto pki server ese-ios-ca grant 2
crypto pki server ese-ios-ca info requests
! Enrollment Request Database:
! ReqID  State      Fingerprint                      SubjectName
! --------------------------------------------------------------------
!  2      granted    0784BC89DE717A105ABD9B2260FE5F53 hostname=ese-branch.ese.cisco.com
dir nvram:
! Directory of nvram:/
!
!    50  -rw-        2570                    <no date>  startup-config
!    51  ----        1924                    <no date>  private-config
!     1  -rw-           0                    <no date>  ifIndex-table
!     2  ----          12                    <no date>  persistent-data
!     3  -rw-         272                    <no date>  ese-ios-ca.pub
!     4  -rw-         963                    <no date>  ese-ios-ca.prv
!     5  -rw-         112                    <no date>  1.cnm
!     6  -rw-          32                    <no date>  ese-ios-ca.ser
!     7  -rw-         300                    <no date>  ese-ios-ca.crl
!     8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
!     9  -rw-          89                    <no date>  2.cnm
!    10  -rw-          89                    <no date>  3.cnm
!
! 57336 bytes total (42550 bytes free)
more nvram:3.cnm
! subjectname_str = hostname=ese-branch.ese.cisco.com
! expiration = 17:10:10 EDT Oct 10 2004
```

Removing the Pre-Shared Key

In previous examples, two routers were enrolled to the Cisco IOS CA: one VPN headend and one VPN branch. Next, remove the pre-shared key from the VPN headend for this branch, clear the IPSec tunnel, and reinitiate the IPSec connection from the branch VPN router. Note that the crypto headend is configured with the dynamic crypto map, so only a branch can initiate a new tunnel connection. To complete this process, perform the following steps:

Step 1 To remove the pre-shared key for the branch that is already enrolled on the VPN headend, enter the following commands:

```
conf
  no crypto isakmp key bigsecret address 66.66.66.2
end
copy run start
  ! Destination filename [startup-confg]?
<return>
  ! Building configuration
  ! [OK]
clear crypto isa
clear crypto sa
```

Note Because DPD is configured on both VPN headend and the VPN branches, the branch side of this IPSec tunnel should clear itself in about 30 seconds. You can validate the status of the IPSec tunnel on either the headend or branch routers by entering the **show crypto isa sa detail** command.

Step 2 To verify the removal of the PSK ISAKMP SA on the VPN branch router, enter the following command:

```
show crypto isa sa detail
  ! Codes: C - IKE configuration mode, D - Dead Peer Detection
  !        K - Keepalives, N - NAT-traversal
  !        X - IKE Extended Authentication
  !        psk - Preshared key, rsig - RSA signature
  !        renc - RSA encryption
  !
  ! C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
```

Step 3 From the branch router LAN interface, ping a host in the private network by entering the following command:

```
ping ip 10.59.138.13 source e0/0 repeat 30
  !
  ! Type escape sequence to abort.
  ! Sending 30, 100-byte ICMP Echos to 10.59.138.13, timeout is 2 seconds:
  ! Packet sent with a source address of 10.113.0.1
  ! .....................!!!!!!!!!!
  ! Success rate is 33 percent (10/30), round-trip min/avg/max = 4/5/8 ms
```

This will initiate an IPSec tunnel. You may have to enter more than one ping while ISAKMP/IKE finishes negotiating the formation of the tunnel.

Step 4 To determine the authentication method that IPSec used, enter the following command:

```
show crypto isa sa detail
  ! Codes: C - IKE configuration mode, D - Dead Peer Detection
  !        K - Keepalives, N - NAT-traversal
  !        X - IKE Extended Authentication
  !        psk - Preshared key, rsig - RSA signature
  !        renc - RSA encryption
  !
  ! C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
  !
  ! 1     66.66.66.2      66.66.66.1               3des sha  rsig 2  23:56:35 D
  !        Connection-id:Engine-id =  1:1(software)
```

The term rsig indicates that a digital certificate was used for authentication.

(Optional) To remove the **crypto isakmp key bigsecret address 66.66.66.1** and **crypto isakmp policy 1** statements enter the "no" form of each command at the branch router. This may speed up the tunnel creation process. However, even if you do not, there is no longer a match for that key on the VPN headend system, so that policy will not be a viable authentication for ISAKMP.

Distributing the CRL over SCEP

A major advantage of deploying digital certificates is the administrative control it gives you over remote connections. The IPSec connections come through a centralized IPSec crypto headend that verifies that the certificate is valid by checking to see if it is on the revocation list (CRL). The branch is only granted access if the certificate is still valid. If the branch certificate has been revoked or has expired, ISAKMP authentication fails and no access is given to the enterprise network.

The following are frequently asked questions about CRLs and the CDP:

Q1. How do CRLs work?

A. The Cisco IOS CA server keeps a list of digital certificate serial numbers that have been administratively revoked. Devices that rely on digital certification to communicate with one another (known as VPN crypto-endpoints), can retrieve a copy of the CRL from the Certificate Distribution Point (CDP). Before communication occurs between VPN crypto endpoints, Any device with **revocation-check crl** enabled determines whether or not to allow communication with the other side of the IPSec VPN based on the CRL and the expiration times.

Any device with **revocation-check crl** enabled determines whether or not a device on the other end of the communication is on the CRL. Devices with revoked certification are not allowed to communicate, do not pass ISAKMP authentication, and no IPSec tunnel (IPSec SA) is established.

Before implementing and deploying a CRL, consider the following design issues:

- CRL distribution time (expiration time), IPSec SA and ISAKMP SA lifetimes—The CRL lifetime affects the length of time the CRL can be used with the VPN devices. The IPSec SA and ISAKMP SA lifetimes affect how long a currently operating VPN IPSec tunnel is allowed to continue to operate before rekeying and checking the CRL.
- Method and location of CRL distribution, called the Certification Distribution Point (CDP)—The method determines how the CRL is fetched, such as using raw HTTP, SCEP, or TFTP. The location determines how the CRL is fetched, including the server and file pathnames.

Q2. How does CRL distribution and the CDP work?

A. On the Cisco IOS CA server, the CDP defaults to SCEP, which occurs over HTTP, for communication between the VPN crypto router and the Cisco IOS CA server. When the router enrolls with the Cisco IOS CA, the certificate that was issued contains a field identifying the CDP from which to fetch the CRL and the protocol to use. If the CDP URL is configured on the Cisco IOS CA trustpoint, then the VPN crypto routers default to using SCEP.

Q3. Can I store the CRL and other CA files on something other than the Cisco IOS CA?

A. Yes. See the "Backing Up and Restoring the Cisco IOS CA Server" section on page 42 for details.

Q4. When is the CRL checked?

A. If the VPN crypto endpoint has the **revocation-check crl** option enabled, during IKE negotiation the serial number of the remote peer certificate is checked against the CRL. If it is on the CRL, IKE authentication fails and no ISAKMP SA is created.

- If two VPN crypto peers are already communicating when the revocation occurs, the current IPSec tunnel continues to work until either the security association (SA) lifetime expires, until an IPSec SA re-key is initiated, or until the administrator manually clears one side of the tunnel, leaving DPD to clear the other side.
- If the VPN crypto endpoint (router) is set to **revocation-check crl none** it never checks or fetches the CRL.

Q5. When is a new copy of the CRL fetched by the VPN crypto endpoint?

A. The events that cause the VPN crypto endpoints to fetch the CRL from the CDP are:

- The CRL lifetime expires. CRL lifetime is an option that can be specified when configuring the Cisco IOS CA server with the **lifetime crl time** command. This command sets the CRL expiration time on the Cisco IOS CA server.
- The administrator issues the **crypto ca crl request trustpoint_name** command on the VPN crypto endpoint to cause this router to immediately request the CRL from the CDP.
- The VPN crypto router is reloaded. After reload has occurred, the router requests the CRL from the CDP.

Q6. How do I administratively view information about the CRL on the Cisco IOS CA server?

A. Use the following command:

```
crypto pki server ese-ios-ca info crl
! Certificate Revocation List:
!     Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
!     This Update: 14:31:24 EST Feb 2 2004
!     Next Update: 14:31:24 EST Feb 3 2004
!    Number of CRL entries: 1
!    CRL size: 322 bytes
! Revoked Certificates:
!    Serial Number: 0x03
!    Revocation Date: 14:31:24 EST Feb 2 2004
```

The highlighted section represents a revoked certificate with serial number 3 (in hexadecimal, this is **0x03**).

Q7. How do I view information about the CRL on the VPN crypto routers that has **revocation-check crl** enabled?

A. Use the following command:

```
show crypto ca crls
! CRL Issuer Name:
! cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
! LastUpdate: 09:58:36 EST Feb 2 2004
! NextUpdate: 09:58:36 EST Feb 3 2004
! Retrieved from CRL Distribution Point:
! ** CDP Not Published - Retrieved via SCEP
```

The following are some considerations regarding the VPN crypto router view of the CRL:

- If the branch VPN router has **revocation check none** or **crl optional** set, it does not fetch the CRL from the CDP, nor does it check the CRL during IKE.
- The **show crypto crls** command only shows basic information such as Name, LastUpdate, and NextUpdate.

Revoking a Digital Certificate for a Branch VPN Router

Consider the following two issues that are important when using CRLs to revoke branch access:

- The CRL is only fetched from the CDP under the following three circumstances:
  - Reboot
  - Manual request
  - Certification expiration
- The CRL is only checked on devices with **revocation-check crl** enabled and only during IKE authentication. Checking does not effect an already active VPN IPSec tunnel unless it is in ISAKMP negotiation, such as re-key or initial tunnel negotiation.

To remove a digital certificate that was issued by the Cisco IOS CA, perform the following steps on the Cisco IOS CA server:

Step 1 Determine the certificate serial number by one of the following methods:

- Make sure the device is on-line and telnet / ssh to the branch you are going to revoke. Either view NVRAM or execute the **show run** command.
- Locate the hostname of the device in the CA server <serial#>.cnm files. The device hostname gives you the serial number. In the example used in this document, the hostname ese.cisco.com has a certificate with the serial number 3, or 03 in hex. Use the **more nvram:3.cnm** command to verify the hostname and certificate expiration date.

```
dir nvram:
    ! Directory of nvram:/
    !
    !   50  -rw-        2570                    <no date>  startup-config
    !   51  ----        1924                    <no date>  private-config
    !   1  -rw-           0                    <no date>  ifIndex-table
    !   2  ----          12                    <no date>  persistent-data
    !   3  -rw-         272                    <no date>  ese-ios-ca.pub
    !   4  -rw-         963                    <no date>  ese-ios-ca.prv
    !   5  -rw-         112                    <no date>  1.cnm
    !   6  -rw-          32                    <no date>  ese-ios-ca.ser
    !   7  -rw-         300                    <no date>  ese-ios-ca.crl
    !   8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
    !   9  -rw-          89                    <no date>  2.cnm
    !   10  -rw-          89                    <no date>  3.cnm
    !
    !   57336 bytes total (42550 bytes free)
```

```
more nvram:3.cnm
    !   subjectname_str = hostname=ese-branch.ese.cisco.com
    !   expiration = 17:10:10 EDT Oct 10 2004
```

Step 2 (Optional) To determine if a certificate has already been revoked, enter the following command:

```
crypto pki server ese-ios-ca info crl
    !   Certificate Revocation List:
    !   Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
    !   This Update: 09:58:36 EST Feb 2 2004
    !   Next Update: 09:58:36 EST Feb 3 2004
    !   Number of CRL entries: 0
    !   CRL size: 300 bytes
```

In this example, the CRL is empty.

Step 3 To revoke the certificate serial number, enter the following command:

```
crypto pki server ese-ios-ca revoke 0x3
```

Note The string "0x" is required before the serial number to indicate that the subsequent number is in hexadecimal. In this example, the serial number is 3, so the complete identifier is **0x3**.

Step 4 To check the Cisco IOS CA server CRL and verify that revocation is successful, enter the following command:

```
crypto pki server ese-ios-ca info crl
    !   Certificate Revocation List:
    !   Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
    !   This Update: 14:31:24 EST Feb 2 2004
    !   Next Update: 14:31:24 EST Feb 3 2004
    !   Number of CRL entries: 1
    !   CRL size: 322 bytes
    !   Revoked Certificates:
    !       Serial Number: 0x03
    !       Revocation Date: 14:31:24 EST Feb 2 2004
```

Step 5 To manually force a fetch of the CRL from the CDP on the VPN crypto headend device (router), enter the following commands:

```
conf t
crypto ca crl request ese-ios-ca
end
```

Step 6 To check the time stamp of the CRL on the VPN crypto headend device (router), enter the following command:

```
show crypto ca crls
    !   CRL Issuer Name:
    !   cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
    !   LastUpdate: 14:31:24 EST Feb 2 2004
    !   NextUpdate: 14:31:24 EST Feb 3 2004
    !   Retrieved from CRL Distribution Point:
        ** CDP Not Published - Retrieved via SCEP
```

Note The **show crypto ca crl** command on the crypto routers does not show the actual items in the CRL. This is only shown by the **show** command on the Cisco IOS CA server.

Step 7 (Optional) Clear the Crypto ISAKMP SA for any current connections to the revoked branch.

Perform these steps if you do not want to wait for a rekey after the IPSec SA lifetime expires.

a. To determine if there is a ISAKMP SA for this branch, enter the following command:

```
show crypto isa sa
    !   conn-id  slot
    !   66.66.66.1     66.66.66.2      QM_IDLE              5    0
```

b. If an ISAKMP SA exists, clear it using the connection ID, as in the following example:

```
clear crypto isa 5
```

c. To determine if the IPSec SA pair is still running, enter the following command:

```
show crypto engine connection active
    !   ID Interface   IP-Address     State      Algorithm  Encrypt  Decrypt
    !   5141 FastEthernet0/0 66.66.66.1set    HMAC_SHA+3DES_56_C        0      104
    !   5142 FastEthernet0/0 66.66.66.1set    HMAC_SHA+3DES_56_C      104        0
```

Step 8 If IPSec SAs are still present, clear them by entering the following command:

```
clear crypto sa peer 66.66.66.2
```

Note Wait at least 30 seconds for DPD to tear down the IPSec tunnel on the branch VPN crypto router.

Examples of Revoked Certificate Logs

If you enable the **debug crypto pki transaction** and **term mon** commands, an explicit message is displayed stating that the certificate was revoked. However, it is recommended that you only run **debug** commands on a router while troubleshooting; never under heavy load on a production headend crypto system.

The following example shows how to clear the ISAKMP SA (connection ID 5) and the associated IPSec SAs. DPD tears down the IPSec SA, after about 30 seconds. The router log entries are stored in the router logging facilities, and can be simultaneously logged to a common log server for permanent storage, if required.

VPN Branch Router

This example illustrates logging with buffered debug and an attempt to initiate a new IPSec tunnel by causing the branch to headend traffic.

```
ese-branch# ping ip 10.59.138.13 source e0/0 repeat 45

Type escape sequence to abort.
Sending 45, 100-byte ICMP Echos to 10.59.138.13, timeout is 2 seconds:
Packet sent with a source address of 10.113.0.1
…..........................................
Success rate is 0 percent (0/45)
ese-branch#
ese-branch# show log
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 5979 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 11 messages logged, xml disabled,
```

```
                    filtering disabled
        Logging to: vty6(11)
    Buffer logging: level debugging, 5979 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
    Trap logging: level informational, 5962 message lines logged

Log Buffer (4096 bytes):

Feb  2 20:56:49.844: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational mode failed
with peer at 66.66.66.1
```

Note Notice in the last line that the ping failed, the branch was unable to successfully get to QM_IDLE in ISAKMP, and it was unable bring up a IPSec Tunnel to the VPN crypto headend router.

VPN Crypto Headend Router

This example illustrates logging with buffered debug and the **show log** command for viewing the branch being blocked.

```
ese-cryagg# show log
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 5692 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 5692 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 5676 message lines logged

Log Buffer (4096 bytes):

Feb  2 20:25:53.923: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 66.66.66.2
is bad: certificate invalid
```

The highlighted log message is what the administrator sees (in the version of the Cisco IOS software used in this example), when a revoked branch attempts to connect to a crypto headend, which finds the branch certificate serial number in the CRL.

Note You can use the **show crypto isa sa** command to see the branch come in and the ISAKMP SA go to MM_KEY_EXCH. It will never get to QM_IDLE.

Copying Certificate Enrollments to a Cisco IOS CA

If you cut and paste the certificate enrollment, you do not need an IPSec prep tunnel. Simply telnet/ssh to the remote router and copy between the enrolling router and the Cisco IOS CA server. This can be used with a device that does not support SCEP to manually enroll it with a Cisco IOS CA server. To manually copy certificate enrollment, perform the following steps:

Step 1 To copy the CA public signing certificate from an enrolled router, enter the following command:

```
crypto ca export ese-ios-ca pem terminal 3des cisco123
  ! % CA certificate:
  ! -----BEGIN CERTIFICATE-----
  ! MIICnzCCAgigAwIBAgIBATANBgkqhkiG9w0BAQQFADBjMQwwCgYDVQQIEwMgTkMx
  ! ETAPBgNVBAcTCCBSYWxlaWdoMRswGQYDVQQKExIgQ2lzY28gU3lzdGVtcyBJbmMx
  ! DTALBgNVBAsTBCBFU0UxFDASBgNVBAMTCyBlc2UtaW9zLWNhMB4XDTA0MDEzMDE0
  ! NTgyMFoXDTA1MDYyMTE0NTgyMFowYzEMMAoGA1UECBMDIE5DMREwDwYDVQQHEwgg
  ! UmFsZWlnaDEbMBkGA1UEChMSIENpc2NvIFN5c3RlbXMgSW5jMQ0wCwYDVQQLEwQg
  ! RVNFMRQwEgYDVQQDEwsgZXNlLWlvcy1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
  ! gYkCgYEAryGYxW8aj1rFAf+t+xSJH1A/kco8P6OfssFQ/8v4FSqnMGDnmvUQ4pLB
  ! ccaAS0UMqtSvWDSrhbIEIIs5YNINm1Gve6zxLT31vG6udxhq6RRx9aREPOW1Ezbs
  ! M1/rM5gALBXun4/TMYNJDYqYP7vhnnKhMBIaO5ejrNFHw32j1ncCAwEAAaNjMGEw
  ! DwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFCbilZWX
  ! zQU/Vz8eISA/6ajii6z7MB8GA1UdIwQYMBaAFCbilZWXzQU/Vz8eISA/6ajii6z7
  ! MA0GCSqGSIb3DQEBBAUAA4GBAHAlE36r2t9uYLVu0W5E7ayGVDN5/ra+UihmoGu8
  ! +OKiwO0Y7mya8wR5BA9OQhjNdMHf4Bsx4nV7emGKffgTGrLmZpj+iVv9DQLOUmKn
  ! /Osyx1k8/iPsKOJDSCGotiQLfigcGlEKxbNNxTNf4UO1IarHG8fY9E9dvs/U/wuU
  ! CQGx
  ! -----END CERTIFICATE-----
  ! % RSA keypair 'ese-cryagg.ese.cisco.com' is not exportable.
```

Note Cut and paste the entire certificate including BEGIN and END lines.

You can copy the certificate from a headend or any other enrolled router except the Cisco IOS CA server. You can keep the certificate for future enrollments and reuse it because it will not change until it expires.

Step 2 To clear trustpoints or crypto keys on the enrolling router, enter the following command and respond to the system prompt:

This removes the certificates. Skip this step if this router has never been configured.

```
no crypto ca trustpoint ese-ios-ca
  ! % Removing an enrolled trustpoint will destroy all certificates
  !  received from the related Certificate Authority.
  !
  ! Are you sure you want to do this? [yes/no]:
yes
  ! % Be sure to ask the CA administrator to revoke your certificates.
  !
  ! No enrollment sessions are currently active.
```

Step 3 To remove the generated public/private key pair that was previously generated, enter the following command and respond to the system prompt:

```
crypto key zeroize rsa
  ! % All RSA keys will be removed.
  ! % All router certs issued using these keys will also be removed.
  ! Do you really want to remove these keys? [yes/no]:
yes
```

Step 4 To set the router time clock manually, enter the **set clock** command. To set it with a time server, enter the **ntp** command.

Certificates have built-in expiration times and must be checked against the system time before they can be used. Setting a hostname makes future enrollment and configuration easier.

```
conf t
    ip hostname ese-branch
    clock timezone EST -5
    clock summer-time EDT recurring
    ip domain name ese.cisco.com
    ip host ese-ios-ca 10.59.138.12
    ntp server 172.26.176.10
!
```

Step 5 To generate a new public/private key pair on the enrolling router, enter the following command:

```
crypto key generate rsa general-keys modulus 1024
  ! The name for the keys will be: ese-branch.ese.cisco.com
  !
  ! % The key modulus size is 1024 bits
  ! % Generating 1024 bit RSA keys ...[OK]
```

Step 6 To create and configure the trustpoint on the enrolling router, enter the following commands:

```
crypto ca trustpoint ese-ios-ca
! The following line allows you to generate a request via the CLI terminal rather than
! via SCEP.
enrollment terminal
revocation-check crl none
source interface Ethernet0/0
auto-enroll 70
!
```

Step 7 To authenticate with CA over a terminal, enter the following command:

```
crypto ca authenticate ese-ios-ca
```

When this step is completed successfully, you receive the CA signing certificate.

Step 8 Paste in the CA signing certificate from Step 1. Then on a new line, type **quit**, press Return, and respond to the system prompt.

```
-----BEGIN CERTIFICATE-----
MIICnzCCAgigAwIBAgIBATANBgkqhkiG9w0BAQQFADBjMQwwCgYDVQQIEwMgTkMx
ETAPBgNVBAcTCCBSYWxlaWdoMRswGQYDVQQKExIgQ2lzY28gU3lzdGVtcyBJbmMx
DTALBgNVBAsTBCBFU0UxFDASBgNVBAMTCyBlc2UtaW9zLWNhMB4XDTA0MDEzMDE0
NTgyMFoXDTA1MDYyMTE0NTgyMFowYzEMMAoGA1UECBMDIE5DMREwDwYDVQQHEwgg
UmFsZWlnaDEbMBkGA1UEChMSIENpc2NvIFN5c3RlbXMgSW5jMQ0wCwYDVQQLEwQg
RVNFMRQwEgYDVQQDEwsgZXNlLWlvcy1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAryGYxW8aj1rFAf+t+xSJH1A/kco8P6OfssFQ/8v4FSqnMGDnmvUQ4pLB
ccaAS0UMqtSvWDSrhbIEIIs5YNINm1Gve6zxLT31vG6udxhq6RRx9aREPOW1Ezbs
M1/rM5gALBXun4/TMYNJDYqYP7vhnnKhMBIaO5ejrNFHw32j1ncCAwEAAaNjMGEw
DwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFCbilZWX
zQU/Vz8eISA/6ajii6z7MB8GA1UdIwQYMBaAFCbilZWXzQU/Vz8eISA/6ajii6z7
MA0GCSqGSIb3DQEBBAUAA4GBAHAlE36r2t9uYLVu0W5E7ayGVDN5/ra+UihmoGu8
+OKiwO0Y7mya8wR5BA9OQhjNdMHf4Bsx4nV7emGKffgTGrLmZpj+iVv9DQLOUmKn
/Osyx1k8/iPsKOJDSCGotiQLfigcGlEKxbNNxTNf4UO1IarHG8fY9E9dvs/U/wuU
CQGx
-----END CERTIFICATE-----
quit
  ! Certificate has the following attributes:
  ! Fingerprint: 9D8D787D 574D2955 CA666B2B 22F3C31A
  ! % Do you accept this certificate? [yes/no]:
yes
```

```
  ! Trustpoint CA certificate accepted.
  ! % Certificate successfully imported
```

Step 9 To start the certificate enrollment request process on the enrolling router, enter the following command and respond to the system prompts:

```
crypto ca enroll ese-ios-ca
  ! % Start certificate enrollment ..
  !
  ! % The fully-qualified domain name in the certificate will be: ese-branch.ese.cisco.com
  ! % The subject name in the certificate will be: ese-branch.ese.cisco.com
  ! % Include the router serial number in the subject name? [yes/no]:
no
  ! % Include an IP address in the subject name? [no]:
no
  ! Display Certificate Request to terminal? [yes/no]:
yes
  ! Certificate Request follows:
  !
  ! MIIBiTCB8wIBADApMScwJQYJKoZIhvcNAQkCFhhlc2UtYnJhbmNoLmVzZS5jaXNj
  ! by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAL2yKsahG2BtSIYlfKFk
  ! Amt6S/MwOYrtASwxEqn1lNk06M/GMpAnupFlFMt+91X/90hxtWQTzqCXRJKKaqSm
  ! YESMX1lO0lNhmuVXmuP/7BFJLuzPq6HCBMqk8GR9rQntnIP7ezssdalpXevOKgE5
  ! xwht3rPsHPSnDx6ZGd5Oy8yHAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1Ud
  ! DwEB/wQEAwIFoDANBgkqhkiG9w0BAQQFAAOBgQBxQLDrhSHyTnw/JoGamd79+qBz
  ! +L1WvVkFsBgAkpuSW6zC+hyxXpVJmkbqEzSgKGdUm6S5jHnVJjPaGfI5w6IptTsI
  ! GXROLDmqdE9fo9BDfMcEPcKBE44bq0ZAKAcu4uaGSsJtD2tie+OVMPTwhYx+kr4t
  ! yGUGKth1V6dRAcw8jw==
  !
  ! ---End - This line not part of the certificate request---

  ! Redisplay enrollment request? [yes/no]:
no
```

Copy the certificate request that is generated by this command for use during the next step. Copy only the lines between “Certificate Request follows” and “---End-“.

Step 10 Enter the following command on the Cisco IOS CA server using a telnet or SSH connection. Grant the request and capture the certificate information for the enrolling router. Paste the information into the command, then type **quit** on a new line and press Return.

```
crypto pki server ese-ios-ca request pkcs10 terminal
  ! % Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
MIIBiTCB8wIBADApMScwJQYJKoZIhvcNAQkCFhhlc2UtYnJhbmNoLmVzZS5jaXNj
by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAL2yKsahG2BtSIYlfKFk
Amt6S/MwOYrtASwxEqn1lNk06M/GMpAnupFlFMt+91X/90hxtWQTzqCXRJKKaqSm
YESMX1lO0lNhmuVXmuP/7BFJLuzPq6HCBMqk8GR9rQntnIP7ezssdalpXevOKgE5
xwht3rPsHPSnDx6ZGd5Oy8yHAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1Ud
DwEB/wQEAwIFoDANBgkqhkiG9w0BAQQFAAOBgQBxQLDrhSHyTnw/JoGamd79+qBz
+L1WvVkFsBgAkpuSW6zC+hyxXpVJmkbqEzSgKGdUm6S5jHnVJjPaGfI5w6IptTsI
GXROLDmqdE9fo9BDfMcEPcKBE44bq0ZAKAcu4uaGSsJtD2tie+OVMPTwhYx+kr4t
yGUGKth1V6dRAcw8jw==
quit
  ! % Enrollment request pending, reqId=3

crypto pki server ese-ios-ca info requests
  ! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------------
  ! 3      pending    D3EB83CEB0C8E2C0DA25EE42DB0155FC
```

Step 11 When you grant the certificate enrollment request on the Cisco IOS CA it will return to the CLI with the enrolling router. The digital certificate follows. Copy this to paste it into the enrolling router later.

```
crypto pki server ese-ios-ca grant 3
  ! % Granted certificate:
  ! MIICNTCCAZ6gAwIBAgIBBDANBgkqhkiG9w0BAQQFADBjMQwwCgYDVQQIEwMgTkMx
  ! ETAPBgNVBAcTCCBSYWxlaWdoMRswGQYDVQQKExIgQ2lzY28gU3lzdGVtcyBJbmMx
  ! DTALBgNVBAsTBCBFU0UxFDASBgNVBAMTCyBlc2UtaW9zLWNhMB4XDTA0MDIwMzE2
  ! NDAwM1oXDTA0MTAxNDE2NDAwM1owKTEnMCUGCSqGSIb3DQEJAhYYZXNlLWJyYW5j
  ! aC5lc2UuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9sirG
  ! oRtgbUiGJXyhZAJrekvzMDmK7QEsMRKp9ZTZNOjPxjKQJ7qRZRTLfvdV//dIcbVk
  ! E86gl0SSimqkpmBEjF9ZTtJTYZrlV5rj/+wRSS7sz6uhwgTKpPBkfa0J7ZyD+3s7
  ! LHWpaV3rzioBOccIbd6z7Bz0pw8emRneTsvMhwIDAQABozMwMTAOBgNVHQ8BAf8E
  ! BAMCBaAwHwYDVR0jBBgwFoAUJuKVlZfNBT9XPx4hID/pqOKLrPswDQYJKoZIhvcN
  ! AQEEBQADgYEAYKpMuZQT3rEirIXlRc9ffhKEQw2fPN776M2/hV9wYYXMpqYVZ+Cl
  ! HTYEg4iAAte5kvkwu741Crp3XJ5+IFBh7fhDj8PJaVmWsN+0puxPquH8fFRC28zt
  ! j4Gcye73vLKPMczz42Q8HxJaPKcZGUYNn8xMyhrINjCyzkLXKjgczgY=
```

Step 12 To confirm that Cisco IOS CA server issued the certificate, enter the following command:

```
dir nvram:
  ! Directory of nvram:/
  !
  !    50  -rw-        2568                    <no date>  startup-config
  !    51  ----        1924                    <no date>  private-config
  !     1  -rw-           0                    <no date>  ifIndex-table
  !     2  ----          12                    <no date>  persistent-data
  !     3  -rw-         272                    <no date>  ese-ios-ca.pub
  !     4  -rw-         963                    <no date>  ese-ios-ca.prv
  !     5  -rw-         112                    <no date>  1.cnm
  !     6  -rw-          32                    <no date>  ese-ios-ca.ser
  !     7  -rw-         322                    <no date>  ese-ios-ca.crl
  !     8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
  !     9  -rw-          89                    <no date>  2.cnm
  !    10  -rw-          89                    <no date>  3.cnm
  !    11  -rw-          89                    <no date>  4.cnm
  !
  ! 57336 bytes total (41528 bytes free)

more nvram:4.cnm
  ! subjectname_str = hostname=ese-branch.ese.cisco.com
  ! expiration = 12:40:03 EDT Oct 14 2004
```

Step 13 Paste the certificate information into the enrolling router as an import certificate.

If successful, this will become the router certificate.

```
crypto ca import ese-ios-ca certificate
  ! % The fully-qualified domain name in the certificate will be: ese-branch.ese.cisco.com
  !
  ! Enter the base 64 encoded certificate.
  ! End with a blank line or the word "quit" on a line by itself
  !
MIICNTCCAZ6gAwIBAgIBBDANBgkqhkiG9w0BAQQFADBjMQwwCgYDVQQIEwMgTkMx
ETAPBgNVBAcTCCBSYWxlaWdoMRswGQYDVQQKExIgQ2lzY28gU3lzdGVtcyBJbmMx
DTALBgNVBAsTBCBFU0UxFDASBgNVBAMTCyBlc2UtaW9zLWNhMB4XDTA0MDIwMzE2
NDAwM1oXDTA0MTAxNDE2NDAwM1owKTEnMCUGCSqGSIb3DQEJAhYYZXNlLWJyYW5j
aC5lc2UuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9sirG
oRtgbUiGJXyhZAJrekvzMDmK7QEsMRKp9ZTZNOjPxjKQJ7qRZRTLfvdV//dIcbVk
E86gl0SSimqkpmBEjF9ZTtJTYZrlV5rj/+wRSS7sz6uhwgTKpPBkfa0J7ZyD+3s7
LHWpaV3rzioBOccIbd6z7Bz0pw8emRneTsvMhwIDAQABozMwMTAOBgNVHQ8BAf8E
BAMCBaAwHwYDVR0jBBgwFoAUJuKVlZfNBT9XPx4hID/pqOKLrPswDQYJKoZIhvcN
AQEEBQADgYEAYKpMuZQT3rEirIXlRc9ffhKEQw2fPN776M2/hV9wYYXMpqYVZ+Cl
HTYEg4iAAte5kvkwu741Crp3XJ5+IFBh7fhDj8PJaVmWsN+0puxPquH8fFRC28zt
j4Gcye73vLKPMczz42Q8HxJaPKcZGUYNn8xMyhrINjCyzkLXKjgczgY=
quit
```

```
  ! % Router Certificate successfully imported
```

Step 14 To verify that the enrolling router has two certificates (one for the CA and one for the router), enter the following command:

```
show crypto ca certificates
  ! Certificate
  !   Status: Available
  !   Certificate Serial Number: 04
  !   Certificate Usage: General Purpose
  !   Issuer:
  !     cn=ese-ios-ca
  !     ou=ESE
  !     o=Cisco Systems Inc
  !     l=Raleigh
  !     st=NC
  !   Subject:
  !     Name: ese-branch.ese.cisco.com
  !     hostname=ese-branch.ese.cisco.com
  !   Validity Date:
  !     start date: 11:40:03 EST Feb 3 2004
  !     end   date: 12:40:03 EDT Oct 14 2004
  !     renew date: 07:52:03 EDT Jul 30 2004
  !   Associated Trustpoints: ese-ios-ca
  !
  ! CA Certificate
  !   Status: Available
  !   Certificate Serial Number: 01
  !   Certificate Usage: Signature
  !   Issuer:
  !     cn=ese-ios-ca
  !     ou=ESE
  !     o=Cisco Systems Inc
  !     l=Raleigh
  !     st=NC
  !   Subject:
  !     cn=ese-ios-ca
  !     ou=ESE
  !     o=Cisco Systems Inc
  !     l=Raleigh
  !     st=NC
  !   Validity Date:
  !     start date: 09:58:20 EST Jan 30 2004
  !     end   date: 10:58:20 EDT Jun 21 2005
  !   Associated Trustpoints: ese-ios-ca
```

Step 15 To change the enrolling router trustpoint back to SCEP for later auto re-enrollment over SCEP, enter the following commands:

```
crypto ca trustpoint ese-ios-ca
 enrollment mode ra
 enrollment url http://ese-ios-ca:80
```

Step 16 To save the configuration on the enrolling router, enter the **copy run start** or **wr mem** command.

```
end
copy run start
  ! Destination filename [startup-config]?
<return>
  ! Building configuration...
  ! [OK]
```

Step 17 To verify that the enrolling router NVRAM has both the CA and its own certificates stored correctly, enter the following command:

```
dir nvram:
  ! Directory of nvram:/
  !
  !    23  -rw-        2859                    <no date>  startup-config
  !    24  ----        1956                    <no date>  private-config
  !     1  -rw-           0                    <no date>  ifIndex-table
  !     2  -rw-         569                    <no date>  ese-ios-ca#6104.cer
  !     3  ----          12                    <no date>  persistent-data
  !     4  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
  !
  ! 29688 bytes total (20725 bytes free)
```

Step 18 To clear the crypto on the enrolling router branch and bring up a new IPSec tunnel using the new digital certificate, enter the following commands:

```
clear crypto isa
clear crypto sa
```

Note Wait at least 30 seconds for DPD to remove the ISAKMP/IPSec SA from the crypto headend.

Step 19 To bring up a new IPSec tunnel using the digital certificate and verify authentication for ISAKMP, enter the following commands:

```
ping ip 10.59.138.13 source e0/0 repeat 45
  ! Type escape sequence to abort.
  ! Sending 45, 100-byte ICMP Echos to 10.59.138.13, timeout is 2 seconds:
  ! Packet sent with a source address of 10.113.0.1
  !   ...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  ! Success rate is 93 percent (42/45), round-trip min/avg/max = 4/4/8 ms

show crypto isa sa detail
  ! Codes: C - IKE configuration mode, D - Dead Peer Detection
  !        K - Keepalives, N - NAT-traversal
  !        X - IKE Extended Authentication
  !        psk - Preshared key, rsig - RSA signature
  !        renc - RSA encryption
  !
  ! C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
  ! 1     66.66.66.2      66.66.66.1               3des sha  rsig 2  23:59:11 D
  !        Connection-id:Engine-id =  1:1(software)
```

Automatically Re-enrolling Expired Certificates Before Expiration

All digital certificates have a built in expiration time that is assigned by the issuing CA server during enrollment. When a digital certificate is used for VPN IPSec authentication of ISAKMP SA (IKE), the communicating device certificate expiration time is checked against the VPN endpoint system time. This ensures that a valid, unexpired certificate is used. It is crucial to set the endpoint internal clock correctly. If NTP or SNTP is not possible on the VPN crypto routers then manually enter the **set clock** command.

The certificate is invalid when the system time is earlier or later than the certificate issue time. The certificate is valid if the system time is equal to or within the period between the time when the certificate was issued and the time when it expires.

The auto-enroll feature lets a currently enrolled router automatically re-enroll with the CA server. When using the **auto-enroll** *variable* command, if *variable* is greater than 10, it is interpreted as the percentage remaining of the certificate lifetime.

The auto-enroll feature makes digital certificates easier to manage and support. For example, if a CA issues thousands of certificates to branch VPN routers at the same time without automatic enrollment, they may all expire around the same time and the branches will then lose connectivity through the IPSec VPNs. If you used the **auto-enroll 70** command**,** each router would automatically re-enroll when 70 percent of the router certificate lifetime has expired.

Unless **grant auto** is used on the CA, the administrator needs to manually grant or reject each re-enrollment request. No administrative action is needed at the enrolling router to start the process, but the CA Server still needs to grant or reject each request unless **grant auto** was enabled. Save the new re-enrolled certificate in the re-enrolling VPN router, when appropriate.

If there are no pending unsaved configuration changes, the new certificate is automatically saved in the NVRAM. If there are pending changes, a **copy run start** command is required to save the changes to the NVRAM, and the new certificate replaces the old.

When a new certificate is issued, the old certificate is still on the CA server, but the NVRAM of the VPN router only contains the new certificate. It is recommended that you let the old certificate expire naturally because manually revoking the older certificate increases the CRL size.

Note Newer versions of automatic enrollment can regenerate the key pairs and save them in a temporary file while the auto enroll occurs over an existing IPSec tunnel using the old key pair. The option is to not default to regenerate key pairs.

The following are frequently asked questions about re-enrolling certificates:

Q1. What happens to a VPN router that is connected with a current IPSec tunnel when its certificate expires and auto-enroll was not specified?

A. The current IPSec tunnel remains connected until the session is terminated or the VPN router attempts to rekey in the IPSec SA lifetime.

Q2. How do I tell when my certificate is going to expire?

A. Issue the **show crypto ca** certificate command on the device in question.The issue date, expiration date, and renewal times are listed in the certificate.

Q3. If the certificate on a Cisco router has expired and I try to initiate an IPSec tunnel, what will the log on the VPN branch and VPN headend display?

A. In the following example, **auto-enroll** and NTP are disabled, and the clock set to a future time past the router certificate lifetime. Then IPSec connection is started. This is not recommended, but is used to demonstrate the logging effect on the VPN head and branch of an expired certificate. It is a multiple step procedure.

1. The first step is to enter the following command:

```
show crypto ca certificates
! Certificate
!   Status: Available
!   Certificate Serial Number: 04
!   Certificate Usage: General Purpose
!   Issuer:
!     cn=ese-ios-ca
!     ou=ESE
!     o=Cisco Systems Inc
```

```
!     l=Raleigh
!     st=NC
!   Subject:
!     Name: ese-branch.ese.cisco.com
!     hostname=ese-branch.ese.cisco.com
!   Validity Date:
!     start date: 11:40:03 EST Feb 3 2004
!     end   date: 12:40:03 EDT Oct 14 2004
!     renew date: 07:52:03 EDT Jul 30 2004
!   Associated Trustpoints: ese-ios-ca
!
! CA Certificate
!   Status: Available
!   Certificate Serial Number: 01
!   Certificate Usage: Signature
!   Issuer:
!     cn=ese-ios-ca
!     ou=ESE
!     o=Cisco Systems Inc
!     l=Raleigh
!     st=NC
!   Subject:
!     cn=ese-ios-ca
!     ou=ESE
!     o=Cisco Systems Inc
!     l=Raleigh
!     st=NC
!   Validity Date:
!     start date: 09:58:20 EST Jan 30 2004
!     end   date: 10:58:20 EDT Jun 21 2005
!   Associated Trustpoints: ese-ios-ca
!
```

2. Then display the system time:

```
show clock
  ! 14:33:51.103 EST Thu Feb 5 2004
```

3. To change the NTP configuration and set the clock to a date later than: 12:40:03 EDT Oct 14 2004, enter the following commands:

Note Do not ever do this to a production system. This example demonstrates the effect of misconfiguration.

```
! config t
! no ntp server 172.26.176.10
! no ntp clock-period 17179910
! crypto ca trustpoint ese-ios-ca
!   no auto-enroll 70
! end
```

4. Notice how the router certificate renew date just went into the past. To view the renewal date, enter the following command.

```
show crypto ca certificates
!  Certificate
!    Status: Available
!    Certificate Serial Number: 04
!    Certificate Usage: General Purpose
!    Issuer:
!      cn=ese-ios-ca
!      ou=ESE
!      o=Cisco Systems Inc
!      l=Raleigh
!      st=NC
!    Subject:
!      Name: ese-branch.ese.cisco.com
!      hostname=ese-branch.ese.cisco.com
!    Validity Date:
!      start date: 11:40:03 EST Feb 3 2004
!      end   date: 12:40:03 EDT Oct 14 2004
!      renew date: 19:00:00 EST Dec 31 1969
!    Associated Trustpoints: ese-ios-ca
!
!  CA Certificate
!    Status: Available
!    Certificate Serial Number: 01
!    Certificate Usage: Signature
!    Issuer:
!      cn=ese-ios-ca
!      ou=ESE
!      o=Cisco Systems Inc
!      l=Raleigh
!      st=NC
!    Subject:
!      cn=ese-ios-ca
!      ou=ESE
!      o=Cisco Systems Inc
!      l=Raleigh
!      st=NC
!    Validity Date:
!      start date: 09:58:20 EST Jan 30 2004
!      end   date: 10:58:20 EDT Jun 21 2005
!    Associated Trustpoints: ese-ios-ca
```

5. Now we purposefully set the clock into the future, beyond the lifetime of the router certificate.

```
end
clock set 02:49:00 Feb 5 2035
show clock
! .02:49:05.799 EST Mon Feb 5 2035
```

6. Attempt to start an IPSec connection from this branch router and notice what happens:

```
ping ip 10.59.138.13 source e0/0 repeat 45

  ! Type escape sequence to abort.
  ! Sending 45, 100-byte ICMP Echos to 10.59.138.13, timeout is 2 seconds:
  ! Packet sent with a source address of 10.113.0.1
  ! .............................................
  ! Success rate is 0 percent (0/45)
```

7. Notice the following lines beginning with “Feb 5” and what the VPN *branch* router logged.

```
show log
  ! Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
```

```
  !                 0 flushes, 0 overruns, xml disabled, filtering disabled)
  !     Console logging: level debugging, 58 messages logged, xml disabled,
  !                      filtering disabled
  !     Monitor logging: level debugging, 0 messages logged, xml disabled,
  !                      filtering disabled
  !     Buffer logging: level debugging, 58 messages logged, xml disabled,
  !                     filtering disabled
  !     Logging Exception size (4096 bytes)
  !     Count and timestamp logging messages: disabled
  !     Trap logging: level informational, 63 message lines logged
  !
  ! Log Buffer (4096 bytes):
  !
  !.Feb  5 07:50:31.071: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from
66.66.66.1is bad: CA request failed!
  !.Feb  5 07:50:31.071: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 66.66.66.1
failed its sanity check or is malformed
  !.Feb  5 07:50:31.091: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational
mode failed with peer at 66.66.66.1
  !.Feb  5 07:51:31.359: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from
66.66.66.1 is bad: CA request failed!
  !.Feb  5 07:51:31.359: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 66.66.66.1
failed its sanity check or is malformed
  !.Feb  5 07:51:31.375: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational
mode failed with peer at 66.66.66.1
```

8. Notice the highlighted lines beginning with “Feb 5” and what the VPN *headend* router logged.

```
show log
  ! Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
  !                 0 flushes, 0 overruns, xml disabled, filtering disabled)
  !     Console logging: level debugging, 6079 messages logged, xml disabled,
  !                      filtering disabled
  !     Monitor logging: level debugging, 265 messages logged, xml disabled,
  !                      filtering disabled
  !     Buffer logging: level debugging, 6079 messages logged, xml disabled,
  !                     filtering disabled
  !     Logging Exception size (4096 bytes)
  !     Count and timestamp logging messages: disabled
  !     Trap logging: level informational, 5806 message lines logged
  !
  ! Log Buffer (4096 bytes):
  !
  ! Feb  5 19:51:15.585: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 66.66.66.2
failed its sanity check or is malformed
  ! Feb  5 19:52:15.871: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 66.66.66.2
failed its sanity check or is malformed
```

Q4. If my router clock is set wrong and my certificate expires, is it permanently expired, or can I simply just configure NTP or use the clock set command to correct it again?

A. Just reset the clock on the router using **set clock** or NTP commands, and the certificate will work again.

Q5. If my VPN router was supposed to re-enroll with the auto-enroll command but failed, will it continue to retry, and for how long?

A. Yes it will continue to retry. Run the **show crypto ca timers** command to see when it will retry. It continues to retry until enrollment completes.

Q6. What happens if the CA Server or VPN router reboots while auto-enroll over SCEP is in progress?

A. If the enrolling router is not rebooted, but the Cisco IOS CA server reboots during an SCEP enrollment, the following occurs:

- In Cisco IOS CA server, the enrollment request stays in pending mode until pending mode times out.
- After pending mode times out the client should retry the enrollment.

If enrolling router reboots, but the Cisco IOS CA server is not rebooted during an SCEP enrollment, then the enrolling router sends the request again to the Cisco IOS CA server when it is back online.

Q7. Will auto-enroll automatically kill my old certificate after I have received a new one?

A. No, the Cisco IOS CA keeps the old certificate log files until expiration or revocation. The enrolled VPN router contains only the new certificate.

Q8. Is there a CLI command to tell me when a certificate will re-enroll on a particular router?

A. Yes, use the **show crypto ca timers** command as shown in the following example.

```
show crypto ca timers
  ! PKI Timers
  ! |175d14:11:34.104
  !   |175d14:11:34.104  RENEW ese-ios-ca
```

In the output above, 175d14:11:34.104 indicates that re-enrollment for this certificate will be attempted in 175 days at 14:13:34 (with the trustpoint ese-ios-ca).

Q9. When I use auto-enroll to automatically re-enroll with my CA server, will the re-enrolling router still have the old certificate stored in its NVRAM?

A. In this case, you have two options:

- If there are no pending unsaved changes, the new certificate is automatically written to the NVRAM, replacing the old certificate.
- If there are pending unsaved changes, then you must enter the **copy run start** command on the enrolling router to save the certificate to the NVRAM and remove the old certificate from the NVRAM.

The Cisco IOS CA server keeps both valid certificates until the old certificate expires or is manually revoked.

Backing Up and Restoring the Cisco IOS CA Server

When the Cisco IOS CA server is the primary authentication mechanism for the X-509 certificates used in all the IPSec tunnels in an enterprise, you must have a plan for backing up and restoring the critical data on the Cisco IOS CA system. This section describes and demonstrates recommended procedures, including the following:

- How to backup the critical files used by the Cisco IOS CA server
- What happens if the Cisco IOS CA server device (the router) has a catastrophic failure and nothing can be recovered—there is no NVRAM, flash, or even slot0 storage devices.
- How to restore the critical files to a replacement system.
- Alternate method for off-system live storage of files used by the Cisco IOS CA to an external server, using TFTP/HTTP.

Backing Up Cisco IOS CA Server Files to a Different System

The best way is to periodically, perhaps daily, TFTP/FTP (binary mode) the files stored on the Cisco IOS CA server filesystem to an external server with tape, CD, or DVD backup facilities. Those critical files that need backup are identified in Table 2.

Table 2 Critical Files to Backup

File	Description
cs-label#6101CA.cer[1]	Cisco IOS CA's signing certificate
cs-label.crl	Cisco IOS CA's CRL
cs-label.prv	Export of Cisco IOS CA's private key
cs-label.pub	Export of Cisco IOS CA's public key
cs-label.ser	Counters for Cisco IOS CA server to keep track of what was "last issue Certificate Serial-number"
startup-confg	The Cisco IOS CA startup configuration
Serialnumber.cnm	One log file per issued certificate (these are not critical but are your only record

1. In the examples in this document *cs-label* is the PKI server and key pair name **ese-ios-ca**.

One way to back up a file is by using the Cisco IOS CA CLI. You can copy the files over FTP, as in the following example:

copy nvram:ese-ios-ca.prv ftp://*username***:***password***@***FTPservername***/***pathname***/ese-ios-ca.prv**

Make sure you give the files the appropriate file/directory permissions, so that FTP can write to them on the external server. You may use a scripting or programming language such as Perl or TCL to script a telnet or SSH session on a fixed schedule. You may also use scripting to copy files from the Cisco IOS CA using SNMP MIBs. It does not matter how you back these files up, as long as you do so regularly. The actual frequency depends on your enterprise requirements.

Recovering From Server Failure

If the Cisco IOS CA completely fails, no new IPSec tunnels are allowed. The following example shows the results of a VPN headend trying to log in to a new IPSec tunnel when the Cisco IOS CA is down.

```
show log
  ! Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
  !                 0 flushes, 0 overruns, xml disabled, filtering disabled)
  !     Console logging: level debugging, 35 messages logged, xml disabled,
  !                      filtering disabled
  !     Monitor logging: level debugging, 0 messages logged, xml disabled,
  !                      filtering disabled
  !     Buffer logging: level debugging, 35 messages logged, xml disabled,
  !                     filtering disabled
  !     Logging Exception size (4096 bytes)
  !     Count and timestamp logging messages: disabled
  !     Trap logging: level informational, 37 message lines logged
  !
  ! Log Buffer (4096 bytes):
  !
```

```
  ! Feb  9 15:48:47.157: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 66.66.66.2 failed
its sanity check or is malformed
  ! Feb  9 15:49:47.139: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 66.66.66.2
is bad: CA request failed!
```

The following example shows the results when a VPN branch tries to log in to a new IPSec tunnel when the Cisco IOS CA is down.

```
show log
  ! Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
  !                 0 flushes, 0 overruns, xml disabled, filtering disabled)
  !     Console logging: level debugging, 105 messages logged, xml disabled,
  !                      filtering disabled
  !     Monitor logging: level debugging, 0 messages logged, xml disabled,
  !                      filtering disabled
  !     Buffer logging: level debugging, 105 messages logged, xml disabled,
  !                     filtering disabled
  !     Logging Exception size (4096 bytes)
  !     Count and timestamp logging messages: disabled
  !     Trap logging: level informational, 63 message lines logged
  !
  ! Log Buffer (4096 bytes):
  ! Feb  9 15:48:47.147: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 66.66.66.1 failed
its sanity check or is malformed
  ! Feb  9 15:48:47.167: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational mode
failed with peer at 66.66.66.1
  ! Feb  9 15:49:47.147: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 66.66.66.1 failed
its sanity check or is malformed
```

In this example, new VPN crypto tunnels will not come up because the VPN crypto headend is checking the CA on each new or rekeyed ISAKMP connection.

Note The choice between security and availability must be determined by your corporate security policy and Cisco makes no recommendations in this regard.

Based on your security policy, if you want to allow connectivity while the Cisco IOS CA is down, you can do *one* of the following:

- Allow all devices with issued certificates (including devices with previously revoked certificates), to communicate by entering the command **revocation-check crl none** on the VPN headend. This allows all previously enrolled branches to communicate. Otherwise, none of your branches can communicate during the outage.
- Use certificate maps and skip certificate revocation to allow some sites to connect. This requires the administrator to have a list of the sites to allow in advance of an outage. A plan such as this is a little more complex, but allows some access and some security during an outage. More information can be found in *Using Certificate ACLs to Ignore Revocation Check and Expired Certificates* at the following website:

  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d33e9.html

To allow connectivity while restoring a Cisco IOS CA, perform the following steps:

Step 1 On the VPN crypto headend system, change the **CRL check** to **CRL check none**.

```
conf t
crypto ca trustpoint ese-ios-ca
  revocation-check crl none
end
```

```
copy run start
  ! Destination filename [startup-config]?
<return>
  ! Building configuration...
  ! [OK]
```

Step 2 On a VPN branch router, initiate a call to trigger a new IPSec tunnel to the headend by entering the following command:

```
ping ip 10.59.138.13 source e0/0 repeat 45
  ! Type escape sequence to abort.
  ! Sending 45, 100-byte ICMP Echos to 10.59.138.13, timeout is 2 seconds:
  ! Packet sent with a source address of 10.113.0.1
  ! ..................!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  ! Success rate is 60 percent (27/45), round-trip min/avg/max = 4/4/8 ms
```

Step 3 On the VPN crypto headend systems, verify that the new IPSec connection is allowed:

```
show crypto isakmp sa detail
  ! Codes: C - IKE configuration mode, D - Dead Peer Detection
  !        K - Keepalives, N - NAT-traversal
  !        X - IKE Extended Authentication
  !        psk - Preshared key, rsig - RSA signature
  !        renc - RSA encryption
  !
  ! C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
  ! 5     66.66.66.1      66.66.66.2               3des sha  rsig 2  23:59:01 D
  !        Connection-id:Engine-id =  5:2(hardware)


show crypto engine connections active
  !   ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
  !    5 FastEthernet0/0 66.66.66.1      set    HMAC_SHA+3DES_56_C        0        0
  ! 5127 FastEthernet0/0 66.66.66.1      set    HMAC_SHA+3DES_56_C        0        0
  ! 5128 FastEthernet0/0 66.66.66.1      set    HMAC_SHA+3DES_56_C        0        0
  ! 5129 FastEthernet0/0 66.66.66.1      set    HMAC_SHA+3DES_56_C        0       27
  ! 5130 FastEthernet0/0 66.66.66.1      set    HMAC_SHA+3DES_56_C       27        0
```

As can be seen from these commands, all non-expired VPN branches can now connect.

Restoring Files To a Replacement Cisco IOS CA Server

This example assumes the following:

- You have the necessary hardware required to replace the Cisco IOS CA router
- You backed up your Cisco IOS CA server configuration and associated files using TFTP or FTP to a host-based server in your network.
- You want to restore the configuration and associated files to NVRAM on the new Cisco IOS CA server device.

Perform the following steps to restore the Cisco IOS CA configuration and associated files to a new Cisco router:

Step 1 Verify that the Cisco IOS software image on the replacement router is the same as the previous image.

If not, copy the same Cisco IOS software image and feature set used in the previous Cisco IOS CA server to the replacement system.

```
dir nvram:
  ! Directory of nvram:/
  !
  !    52  -rw-        2146                    <no date>  startup-config
  !    53  ----          24                    <no date>  private-config
  !     1  -rw-           0                    <no date>  ifIndex-table
  !     2  ----          12                    <no date>  persistent-data
  !
  ! 57336 bytes total (53066 bytes free)
```

Step 2 If needed, configure the replacement Cisco IOS CA server to get enough network bandwidth to copy files using TFTP or FTP to the replacement system.

Step 3 Make sure you can successfully ping the IP address of the TFTP/FTP server.

Step 4 Use TFTP or FTP to copy the backup Cisco IOS CA server startup configuration to the replacement Cisco IOS CA server.

a. copy tftp://*TFTP_server_address***/startup-confg startup**

This command copies the backup startup-config to nvram:startup-confg

Note If using FTP, make sure it is in binary mode.

Step 5 To reload the Cisco IOS CA server without saving the current configuration, enter the following commands:

```
end
reload
  ! System configuration has been modified. Save? [yes/no]:
no
  ! Proceed with reload? [confirm]
<return>
```

Do *not* issue a **copy run start** or **wr mem** at this time. This step loads the backup configuration from NVRAM.

Note You already copied the backup startup-config to nvram:, so the old config with the trustpoint and certificates will be loaded on reload.

Step 6 After reboot, log into the router.

Wait at least two minutes for NTP to synchronize and the Cisco IOS CA server to generate files to the NVRAM. It autocreates the *cs-label*.ser, *cs-label*.crl, and the 1.cnm files.

Step 7 To confirm that the process is complete, enter the following command and note the highlighted results:

```
dir nvram:
  ! Directory of nvram:/
  !
  !    50  -rw-        2568                    <no date>  startup-config
  !    51  ----        1920                    <no date>  private-config
```

```
  !     1  -rw-           0                    <no date>  ifIndex-table
  !     2  ----          13                    <no date>  persistent-data
  !     3  -rw-         111                    <no date>  1.cnm
  !     4  -rw-          32                    <no date>  ese-ios-ca.ser
  !     5  -rw-         300                    <no date>  ese-ios-ca.crl
  !
  ! 57336 bytes total (47676 bytes free)
```

Step 8 To remove Cisco IOS CA (PKI) server configuration, enter the following commands and respond to the system prompts as shown:

```
conf t
no crypto pki server ese-ios-ca
  ! % This will stop the Certificate Server process and delete the server configuration
  ! Are you sure you want to do this? [yes/no]:
yes
  ! % Do you also want to remove the associated trustpoint and signing certificate and
key? [yes/no]:
yes
  ! No enrollment sessions are currently active.
  !
  ! % Certificate Server Process stopped
```

Step 9 Use TFTP or FTP to copy the following files to the replacement router NVRAM:

- *cs-label*.pub
- *cs-label*.prv
- *cs-label*.ser
- *cs-label*.crl,
- *cs-label*#6101CA.cer,
- any *serialnum*.cnm files that exist

Enter **copy tftp: nvram:** until all the backed up files are returned to the location they occupied before the failure. You may need to do this file by file. Wildcards (*) in file names are not permitted in router **copy tftp: nvram:** commands. If you use FTP, make sure it is in binary mode.

Note DO overwrite any copies that may already be present.

Step 10 To confirm that all the files are present on the storage device, enter the following command:

```
dir nvram:
  ! Directory of nvram:/
  !
  !    50  -rw-        2568                    <no date>  startup-config
  !    51  ----        1920                    <no date>  private-config
  !     1  -rw-           0                    <no date>  ifIndex-table
  !     2  ----          13                    <no date>  persistent-data
  !     3  -rw-         112                    <no date>  1.cnm
  !     4  -rw-         272                    <no date>  ese-ios-ca.pub
  !     5  -rw-         362                    <no date>  ese-ios-ca.crl
  !     6  -rw-         963                    <no date>  ese-ios-ca.prv
  !     7  -rw-          32                    <no date>  ese-ios-ca.ser
  !     8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
  !     9  -rw-          89                    <no date>  2.cnm
  !    10  -rw-          89                    <no date>  3.cnm
  !    11  -rw-          89                    <no date>  4.cnm
  !    12  -rw-          89                    <no date>  5.cnm
  !    13  -rw-          89                    <no date>  6.cnm
  !
```

```
  ! 57336 bytes total (39484 bytes free)
```

Step 11 To import your public/private key pairs files to the Cisco IOS CA server, enter the following commands:

```
conf t
crypto key import rsa ese-ios-ca pem url nvram: cisco123
  ! % Importing public key or certificate PEM file...
  ! Source filename [ese-ios-ca.pub]?
<return>
  ! Reading file from nvram:ese-ios-ca.pub
  !
  ! % Importing private key PEM file...
  ! Source filename [ese-ios-ca.prv]?
<return>
  ! Reading file from nvram:ese-ios-ca.prv% Key pair import succeeded.
```

You must remember the password that you protected these keys with when you exported them. In the example used in this document, the passphrase is cisco123.

Note Without the correct password, the router will not allow the key pairs to be reimported, and the restore will fail.

Step 12 Manually configure the CA trustpoint to use the key pair and CA certificates key-chain for the original CA signing certificate.

a. To configure the trustpoint, enter the following commands:

```
crypto ca trustpoint ese-ios-ca
revocation-check crl
rsakeypair ese-ios-ca
```

This is done automatically when you create a PKI server, but must be done manually on a restore.

b. To configure the CA signing certificates location, enter the following commands:

```
crypto ca certificate chain ese-ios-ca
certificate ca 01 nvram:ese-ios-ca#6101CA.cer
```

In NVRAM the file is named *cs-label*#6101CA.cer.

Step 13 To reconfigure the Cisco IOS CA (PKI) server, enter the following commands:

```
crypto pki server ese-ios-ca
database level names
database url nvram:
issuer-name CN = ese-ios-ca, OU = ESE, O = Cisco Systems Inc, L = Raleigh, ST = NC, C =
US, EA = ese-vpn-team
lifetime crl 24
lifetime certificate 254
lifetime ca-certificate 508
no shutdown
  ! % Once you start the server, you can no longer change some of
  ! % the configuration.
  ! Are you sure you want to do this? [yes/no]:
yes
  ! % Certificate Server enabled.
end
```

Step 14 To save your configuration to NVRAM on the Cisco IOS CA server, enter the following command:

```
copy run start
  ! Destination filename [startup-config]?
<return>
```

```
! Building configuration...
! [OK]
```

Step 15 To confirm that the Cisco IOS CA server is backed-up and running with the correct last certificate number, enter the following command:

```
show crypto pki server
! Certificate Server status: enabled, configured
!     Granting mode is: manual
!     Last certificate issued serial number: 0x6
!     CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
!     CRL NextUpdate timer: 17:31:05 EST Feb 9 2004
!     Current storage dir: nvram:
!     Database Level: Names - subject name data written as <serialnum>.cnm
```

You should see that the CRL is restored and the CA signing certificate has the original creation date as the start date. Notice that in this example, the last certificate serial number issued is 6.

Step 16 To verify that the previously revoked certificates are back on the CRL, enter the following command:

```
crypto pki server ese-ios-ca info crl
! Certificate Revocation List:
!     Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
!     This Update: 17:31:05 EST Feb 8 2004
!     Next Update: 17:31:05 EST Feb 9 2004
!     Number of CRL entries: 3
!     CRL size: 362 bytes
! Revoked Certificates:
!     Serial Number: 0x03
!     Revocation Date: 14:31:24 EST Feb 2 2004
!     Serial Number: 0x05
!     Revocation Date: 17:19:20 EST Feb 5 2004
!     Serial Number: 0x04
!     Revocation Date: 17:30:56 EST Feb 5 2004
```

Step 17 To verify that the “Start Date” is the date and time that the CA signing Certificate was created, enter the following command:

```
show crypto ca certificates
! CA Certificate
!   Status: Available
!   Certificate Serial Number: 01
!   Certificate Usage: Signature
!   Issuer:
!     cn=ese-ios-ca
!     ou=ESE
!     o=Cisco Systems Inc
!     l=Raleigh
!     st=NC
!   Subject:
!     cn=ese-ios-ca
!     ou=ESE
!     o=Cisco Systems Inc
!     l=Raleigh
!     st=NC
!   Validity Date:
!     start date: 09:58:20 EST Jan 30 2004
!     end   date: 10:58:20 EDT Jun 21 2005
!   Associated Trustpoints: ese-ios-ca
```

Step 18 To verify that all the appropriate files are on the NVRAM storage device, enter the following command:

```
dir nvram:
```

```
! Directory of nvram:/
!
!    50  -rw-        2568                    <no date>  startup-config
!    51  ----        1920                    <no date>  private-config
!     1  -rw-           0                    <no date>  ifIndex-table
!     2  ----          13                    <no date>  persistent-data
!     3  -rw-         112                    <no date>  1.cnm
!     4  -rw-         272                    <no date>  ese-ios-ca.pub
!     5  -rw-         362                    <no date>  ese-ios-ca.crl
!     6  -rw-         963                    <no date>  ese-ios-ca.prv
!     7  -rw-          32                    <no date>  ese-ios-ca.ser
!     8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
!     9  -rw-          89                    <no date>  2.cnm
!    10  -rw-          89                    <no date>  3.cnm
!    11  -rw-          89                    <no date>  4.cnm
!    12  -rw-          89                    <no date>  5.cnm
!    13  -rw-          89                    <no date>  6.cnm
!
! 57336 bytes total (39484 bytes free)
```

You have completed restoring your Cisco IOS CA server. It is back online and will now continue issuing certificates where it left off. If you had enrollments that were pending approval they will need to be reinitiated. Enrollments and revocations that have taken place since these backup file were captured will need to be re-revoked.

Step 19 (Optional) If you disabled CRL checking on the VPN crypto headend during this restore, re-enable CRL checking on the VPN crypto headend.

```
conf t
crypto ca trustpoint ese-ios-ca
  revocation-check crl
end
copy run start
  ! Destination filename [startup-config]?
<return>
  ! Building configuration...
  ! [OK]
clear crypto isakmp
clear crypto sa
```

Re-enabling CRL checking uses the restored copy of the CRL. Routers with previously revoked certificates are no longer able to connect. Approved branches should now be connecting and the VPN crypto headend should be checking the CRL as usual.

Using TFTP/HTTP Server for Off-System Storage of CA Files

You may optionally choose to store the CA signing certificate, the .cnm log files, and the CRL file on an external server on the internal network instead of locally in the Cisco IOS CA server filesystem.

The advantages and disadvantages are described in Table 3.

Table 3 Advantages and Disadvantages of Using TFTP/HTTP for Off-System Storage

Advantages	Disadvantages
• The CA files are kept on a different server that can be easily backed up by the normal server backup process. • An external server provides more storage space for Cisco IOS CA files compared to a "flash" or "disk" card in the Cisco IOS CA. This extra space may be necessary in larger deployments.	• If the TFTP/HTTP server is down then new enrollments may fail, and fetching the CRL from the CDP may fail. This will cause the headend VPN system to prevent IPSec connections. • If a *serialnum*.cnm file was not pre-created for a particular enrollment then that enrollment may fail.

If the TFTP/HTTP server and Cisco IOS CA are in the same location and a site failure occurs, both could be destroyed. If the TFTP/HTTP server is in a different physical location, the communication between the Cisco IOS CA and the TFTP/HTTP server may potentially be over a WAN circuit and more likely to have lower bandwidth or QoS issues.

Note With Cisco IOS software Version 12.4(T), a "split database" feature will be available for the Cisco IOS CA server. This will allow mission-critical files to be stored on the Cisco IOS CA server filesystem, while log files, which are not critical for operation, can be stored externally on a different server. This new feature overcomes most of the disadvantages of off-system storage and give the CA administrator the best of both worlds. The examples in this document do not illustrate the split database feature because it is not yet available at the time that this document is being written.

The following example assumes that a UNIX server running Solaris 8 is on the network with both a TFTP and HTTP daemon pointed to the same directory, with appropriate file permissions granted.

Note On most UNIX systems, you need to pre-create the file and assign the proper ownership and file permissions before you can configure the Cisco IOS CA server. This includes pre-creating the *serialnum*.cnm files.

To enable off-system storage of CA files on a UNIX server, perform the following steps:

Step 1 Configure the UNIX server:

a. Create a file for the TFTP/HTTP solution. Make sure the TFTP daemon and HTTP daemon both have the required directory in the path.

b. Change directories to the TFTP root and execute the following UNIX commands:

```
mkdir certs
cd certs
touch 1.cnm
touch 2.cnm
touch 3.cnm
touch ese-ios-ca#6101CA.cer
touch ese-ios-ca.crl
touch ese-ios-ca.prv
touch ese-ios-ca.pub
touch ese-ios-ca.ser
touch startup-confg
```

```
chmod ugo+ rwx *
```

Step 2 On the Cisco IOS CA server, perform the following steps:

a. Complete preparatory configuration, generate the keys, and export the keys to NVRAM as described in the "Configuring the Cisco IOS CA Server" section on page 6.

b. Add an additional host command to the TFTP/HTTP server on the Cisco IOS CA. For example:

```
ip host harry.cisco.com 172.26.176.10
```

c. Create an alternate Cisco IOS CA configuration to support this off-system storage, such as in the following example:

```
!
crypto pki server ese-ios-ca
  database level names
  database url tftp://harry.cisco.com/vpn/certs
  ! The recommended crl lifetime is 24 hours.
  lifetime crl 24
    ! The recommended certificate lifetime is 2 years (750 days), depending on your
    ! Enterprise's Security policy
  lifetime certificate 750
    ! The recommended ca certificate lifetime is 3 to 5 years (5 years = 1825 days),
    ! depending on your Enterprise's Security policy
  lifetime ca-certificate 1825
  issuer-name CN = ese-ios-ca, OU = ESE, O = Cisco Systems Inc, L = Raleigh, ST = NC,
C = US, EA = ese-vpn-team
    ! the following line shows the web (HTTP) path through the web daemon to the same
    ! directory that the tftp path was mounted on.
  cdp-url  http://harry.cisco.com/solutions/vpn/tftpboot-vpn/certs/ese-ios-ca.crl
    ! "grant auto" may or may not be acceptable in your environment consult you !
    ! security policy before configuring.
  grant auto
  yes
  no shutdown
  yes
!
```

Because the PKI server has **no shutdown** enabled, it creates its files over TFTP to the root of the TFTP/HTTP server.

Note Ensure that both the Cisco IOS CA server and all enrolled devices have access to the external server data or this configuration will not work.

Step 3 Save your certificate on the Cisco IOS CA server:

```
end
copy run start
  ! Destination filename [startup-config]?
<return>
  ! Building configuration...
  ! [OK]
```

Step 4 When the **no shutdown** is completed on the trustpoint in the Cisco IOS CA server, the UNIX TFTP/HTTP server will have written the following files:

```
total 6
-rwxrwxrwx   1 sochmans vpn          111 Feb 10 10:17 1.cnm
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 2.cnm
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 3.cnm
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 ese-ios-ca#6101CA.cer
```

```
-rwxrwxrwx   1 sochmans vpn          300 Feb 10 10:17 ese-ios-ca.crl
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 ese-ios-ca.prv
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 ese-ios-ca.pub
-rwxrwxrwx   1 sochmans vpn           32 Feb 10 10:17 ese-ios-ca.ser
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 startup-confg
```

Step 5 On the Cisco IOS CA server, manually TFTP the following files from the Cisco IOS CA to the TFTP server.

Note In this example the TFTP/HTTP server is named harry.cisco.com and the *cs-label* is ese-ios-ca.

Entering the TFTP commands is a one-time event so that the data for restoring is also copied to the TFTP/HTTP server location.

```
copy start  tftp://harry.cisco.com/vpn/certs/startup-confg
<return>
<return>
copy nvram:ese-ios-ca#6101CA.cer tftp://harry.cisco.com/vpn/certs/ese-ios-ca#6101CA.cer
<return>
<return>
copy nvram:ese-ios-ca.pub tftp://harry.cisco.com/vpn/certs/ese-ios-ca.pub
<return>
<return>
copy nvram:ese-ios-ca.prv tftp://harry.cisco.com/vpn/certs/ese-ios-ca.prv
<return>
<return>
```

Step 6 The following files have now been written on the UNIX TFTP/HTTP server.

```
sochmans@magna% ls -l
total 20
-rwxrwxrwx   1 sochmans vpn          111 Feb 10 10:17 1.cnm
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 2.cnm
-rwxrwxrwx   1 sochmans vpn            0 Feb 10 10:17 3.cnm
-rwxrwxrwx   1 sochmans vpn          675 Feb 10 10:20 ese-ios-ca#6101CA.cer
-rwxrwxrwx   1 sochmans vpn          300 Feb 10 10:17 ese-ios-ca.crl
-rwxrwxrwx   1 sochmans vpn          963 Feb 10 10:19 ese-ios-ca.prv
-rwxrwxrwx   1 sochmans vpn          272 Feb 10 10:19 ese-ios-ca.pub
-rwxrwxrwx   1 sochmans vpn           32 Feb 10 10:25 ese-ios-ca.ser
-rwxrwxrwx   1 sochmans vpn         2727 Feb 10 10:22 startup-confg
```

Step 7 Proceed with enrolling headend or branch VPN routers as usual, except add the following **ip host** statement to their configurations:

```
ip host harry.cisco.com 172.26.176.10
```

The branch still enrolls and authenticates with the Cisco IOS CA server directly, only the CRL Distribution Point (CDP) has been changed in this configuration. The enrolled certificates point directly to the URL for the TFTP/HTTP server but this is done within the certificate issued by the CA.

Observe that the *serialnum*.cnm file is written from the Cisco IOS CA server to the off-system storage server using TFTP/HTTP as each headend/branch enrolls or re-enrolls. The VPN router enrolls with the Cisco IOS CA. If TFTP is the creation mechanism, make sure you pre-create the *serialnum*.cnm files because most UNIX TFTP daemons will not create a new file, but will only update an existing file.

Useful Commands

This section provides examples of commands that are useful when configuring and managing a Cisco IOS CA. It includes the following topics:

Commands for Managing the Cisco IOS CA Server

This section provides examples of commands that can be used for managing the Cisco IOS CA server. It includes the following topics:

Viewing Issued Certificates

To view issued certificates, enter the **dir** command for the location of the certificate storage. In this example that is **NVRAM.**

```
dir nvram:
  ! Directory of nvram:/
  !
  !   50  -rw-        2148                    <no date>  startup-config
  !   51  ----        1924                    <no date>  private-config
  !    1  -rw-           0                    <no date>  ifIndex-table
  !    2  ----          12                    <no date>  persistent-data
  !    3  -rw-         272                    <no date>  ese-ios-ca.pub
  !    4  -rw-         963                    <no date>  ese-ios-ca.prv
  !    5  -rw-         112                    <no date>  1.cnm
  !    6  -rw-          32                    <no date>  ese-ios-ca.ser
  !    7  -rw-         300                    <no date>  ese-ios-ca.crl
  !    8  -rw-         675                    <no date>  ese-ios-ca#6101CA.cer
  !
  ! 57336 bytes total (43574 bytes free)
```

Note The highlighted file, 1.cnm, is the log file for the CA's self signed public certificate (ese-ios-ca#6101CA.cer).

Viewing Certificate Information

Use the **more nvram:1.cnm** command o view the information about each certificate issued by a the CA and stored in the file 1.cnm. This file name (1.cnm) contains the serial number (1) of the certificate to view. This example uses “database level names” logging level and lists:

subjectname_str	Lists the device name
expiration	Lists the expiration date of certificate with serial number 1.

```
more nvram:1.cnm
 ! subjectname_str = cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
 ! expiration = 10:58:20 EDT Jun 21 2005
```

Viewing a Certificate

```
show crypto ca certificates
  ! CA Certificate
  !  Status: Available
  !  Certificate Serial Number: 01
  !  Certificate Usage: Signature
  !  Issuer:
  !    cn=ese-ios-ca
  !    ou=ESE
  !    o=Cisco Systems Inc
  !    l=Raleigh
  !    st=NC
  !  Subject:
  !    cn=ese-ios-ca
  !    ou=ESE
  !    o=Cisco Systems Inc
  !    l=Raleigh
  !    st=NC
  !  Validity Date:
  !    start date: 09:58:20 EST Jan 30 2004
  !    end   date: 10:58:20 EDT Jun 21 2005
  !  Associated Trustpoints: ese-ios-ca
```

Viewing a Key Pair

```
show crypto key mypubkey rsa
  !% Key pair was generated at: 09:28:16 EST Jan 30 2004
  !Key name: ese-ios-ca
  ! Usage: General Purpose Key
  ! Key is exportable.
  ! Key Data:
  !  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198
  !  C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060
  !  E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B
  !  ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE
  !  9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001
  !% Key pair was generated at: 09:28:17 EST Jan 30 2004
  !Key name: ese-ios-ca.server
  ! Usage: Encryption Key
  ! Key is exportable.
  ! Key Data:
  !  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5
  !  0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9
```

```
!  18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2
!  3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001
```

Viewing the Certificate Revocation List

```
crypto pki server ese-ios-ca info crl
  ! Certificate Revocation List:
  !    Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
  !    This Update: 09:58:27 EST Jan 30 2004
  !    Next Update: 09:58:27 EST Jan 31 2004
  !    Number of CRL entries: 0
  !    CRL size: 300 bytes
```

Showing Pending Enrollment Requests

```
crypto pki server ese-ios-ca info requests
  ! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------------
```

Showing Current PKI Server State

```
show crypto pki server
  ! Certificate Server status: enabled, configured
  !    Granting mode is: manual
  !    Last certificate issued serial number: 0x1
  !    CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
  !    CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
  !    Current storage dir: nvram:
  !    Database Level: Names - subject name data written as <serialnum>.cnm
```

See the "Enrollment with a Cisco IOS Software CA Over SCEP" section on page 13 for examples of how to manually grant or reject an enrollment request. If the Cisco IOS CA server is configured for **grant auto** then the CA automatically grants enrollment requests.

Commands for Managing the PKI Server in the Cisco IOS CA Server

The following commands can be used to manage the PKI server in the Cisco IOS CA server.

Command	Description
crypto pki server *cs-label* **grant** {**all** | *tranaction-id*}	Grants all or specific SCEP requests
crypto pki server *cs-label reject* {**all** | *tranaction-id*}	Rejects all SCEP requests.

crypto pki server *cs-label* **password generate** [*minutes*]	Generates a one time password for SCEP request. The password is valid for the number of minutes specified in [minutes]. The valid range is from 1-1440 minutes. The default is 60 minutes. Only one password is valid at a time. If a second password is generated, the previous one is no longer valid.
crypto pki server *cs-label* **revoke** *certificate-serial-number*	Revokes a certificate based on it serial number.
crypto pki server *cs-label* **request pkcs10** {**url** *url* | **terminal**} [**pem**]	Manually adds either base64 or PEM PKCS10 certificate enrollment request to the request database.
crypto pki server *cs-label* **info crl**	Displays information about the status of the current CRL.
crypto pki server *cs-label* **info request**	Displays all outstanding certificate enrollment requests.

Debugging and Troubleshooting Commands

This section lists commands that can be used for debugging and troubleshooting. It includes the following topics:

Debug Commands on the Cisco IOS CA Server

These commands are PKI server related. You will need to issue a terminal monitor if connecting with telnet or ssh.

Command	Description
debug crypto pki messages	Displays the details of the interaction (message dump) between the CA and the router
debug crypto pki server	Displays debugging for a crypto PKI certificate server
debug crypto pki transactions	Displays the interaction (message type) between the CA and the router

For details, see the following website:
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a0080305b65.html#50954

Show Commands on Cisco IOS Crypto Endpoints

These commands are for both headend or branch.

Command	Description
show crypto isa sa	Shows an overview of ISAKMP SAs.
show crypto isa sa detail	Shows details of ISAKMP SAs, such as DPD, NatT, and Auth type.
show crypto engine connection active	Shows an overview of the packets counted on each IPSec SA.
show crypto ipsec sa	Shows an overview of the IPSec SA database.
show crypto ipsec sa detail	Shows detail about each IPSec SA in the SA database.
show crypto eli	Shows counters for the number of IKE sessions.
show crypto session detail	Shows detail of interface and what is applied to the session.
show crypto ca certificates	Shows a readable form of digital certificates installed on this router.
show crypto key mypubkey rsa	Shows crypto key pair and whether or not the key is exportable.
show crypto ca timers	Shows time left before auto-enroll attempts to re-enroll.
show crypto ca crls	Shows the last and next times that the CRL is scheduled to be pulled from the CDP.
show crypto ca trustpoints	Shows basic information about trustpoints configured on this router.
show access-list	Shows access-list counters tied to the Static crypto map.
clear crypto isakmp	Clears all ISAKMP SAs.
clear crypto sa	Clears all IPSec SAs.

Debug Commands on Cisco IOS Software Crypto Endpoints

These commands are for both headend or branch. To see the debugging output, issue a **terminal monitor** command if telnet/ssh was used to connect to the router.

Command	Description
debug crypto pki messages	Displays the details of the interaction (message dump) between the CA and the router
debug crypto pki server	Display debugging for a crypto PKI certificate server
debug crypto pki transactions	Displays the interaction (message type) between the CA and the router
debug crypto isakmp	Displays messages about ISAKMP and IKE events
debug crypto ipsec	Displays IPSec events
debug crypto engine	Displays debug messages about crypto engines, which perform encryption and decryption

For details, see the following website:
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a0080305b65.html#50954

Glossary

Term	Definition
certificate	See X.509 Digital Certificate.
Certificate Authentication	The process of an IPSec network device authenticating to the CA server and if successful receiving the CA server signature certificate.
Certificate Authority	A service responsible for managing certificate requests and issuing certificates to participating IPSec network devices. This service is explicitly entrusted by the receiver to validate identities and to create digital certificates. This service provides centralized key management for the participating devices.
CA	See Certificate Authority.
Certificate Enrollment	The process of an IPSec network device requesting and receiving a digital certificate for itself for use in an IPSec VPN or as identification in any authentication process.
Certificate Revocation	The process of revoking a digital certificate from a IPSec network devices that this CA server had previously enrolled. IPSec network devices with revoked certificates have their certificate's serial number listed on the Certificate Revocation List.
Certificate Revocation List	The Certificate Revocation List is a list of certificate serial numbers, in HEX, that are no longer approved and identifiable by the CA server. Certificate serial numbers listed on the CRL should not pass an authentication process. The CRL is fetched by the enrolled IPSec network devices from the CRL Certification Point.
CRL	See Certificate Revocation List.
CRL Distribution Point	The CDP is the network location and protocol for fetching the CRL from an IPSec network device.
CDP	See CRL Distribution Point.
Dead Peer Detection	This feature uses "keepalive" IKE messages to determine if an IPSec Network device peer is no longer present then removes the SA tunnels that corresponded to that peer. Defined by rfc3706. See http://www.rfc-editor.org/rfc/rfc3706.txt.
DPD	See Dead Peer Detection.

Term	Definition
Internet Key Exchange Protocol	Defined by rfc2409 (http://www.rfc-editor.org/rfc/rfc2409.txt). A key management protocol standard which is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) In context, an entry kept locally in the crypto endpoint device that correlates to this specific tunnel.
IKE	See Internet Key Exchange Protocol.
Internet Security Association Key Management Protocol	The ISAKMP process that occurs prior to the creating the IPSec Tunnel. During this ISAKMP process the two IPSec network devices, authenticate each other via IKE, and then negotiate security parameters that will be used for the IPSec SA for transport of packets between these IPSec network devices. Defined by rfc2408. See http://www.rfc-editor.org/rfc/rfc2408.txt.
ISAKMP	See Internet Security Association Key Management Protocol.
IPSec	See IP Security Protocol Tunnel
IP Security Protocol Tunnel	An IPSec cryptographic tunnel that provides data encryption, digital certificate authentication of cryptographic endpoints, anti-replay and “man in the middle” protection. Defined by RFC 2401. See http://www.rfc-editor.org/rfc/rfc2401.txt.
IPSec crypto tunnel	Generic term used to represent a Virtual Private Network connection between two IPSec network devices.
Tunnel	See IPSec crypto tunnel or IP Security Protocol Tunnel.
Reverse Route Injection	Allows an IPSec network device (usually a crypto headend in a hub-and-spoke topology) to automatically create a static network route in that it’s routing table for each IPSec SA type of connecting IPSec peer device. This network route information is taken from the remote identity of the IPSec SA. This static route may then be redistributed into a dynamic routing protocol if desired.
RRI	See Reverse Route Injection.
Security Association	An instance of security policy and keying material applied to a data flow. Both ISAKMP and IPSec use SAs, although SAs are independent of one another. IPSec SAs are unidirectional and they are unique in each security protocol. An ISAKMP SA is used by IKE only, and unlike the IPSec SA, it is bi-directional. ISAKMP negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually. A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

Term	Definition
SA	See Security Association.
Simple Certificate Enrollment Protocol	A communication protocol used to allow an IPSec network device to enroll with a CA server and receive a digital certificate in a scalable efficient manner. Defined by IETF document. See http://www.ietf.org/internet-drafts/draft-nourse-scep-09.txt.
SCEP	See “Simple Certificate Enrollment Protocol”.
Virtual Private Network	A logical concept that describes a private network over a non-secure network. A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.
VPN	See Virtual Private Network.
X.509 Digital Certificate	Definition: A Digital Certificate for use in authentication and cryptographic purposes. A digital certificate provides identity of a device, cryptographic keying material, and facilitates the digital signature process.

Related Documents

This section contains links to other internal Cisco documentation and other public sources about VPN related ESE material.

- *Business Ready Teleworker SRND*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79d.pdf
- *Enterprise Class Teleworker Solution Reference Network Design Guide*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79d.pdf
- *Voice and Video Enabled IPSec VPN (V3PN) Solution Reference Network Design Guide*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- *Cisco AVVID Network Infrastructure Data-only Enterprise Site-to-Site VPN Design Solutions Reference Network Design*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns142/c649/ccmigration_09186a00801e12ca.pdf