Cisco Systems
Networking Academy

Cisco.com

Network Security 2

Module 5 – Configure Site-to-Site VPNs Using Digital Certificates

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

Cisco Systems Networking Academy

Cisco.com

Module 5 – Configure Site-to-Site VPNs Using Digital Certificates

5.1 Configure CA Support on a Cisco Router

CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

Cisco IOS Software CA Configuration Procedure

Cisco.com

- Step 1 – (Optional) Manage the NVRAM memory usage.
- Step 2 – Set the router time and date.
  `clock timezone`
  `clock set`
- Step 3 – Configure the router hostname and domain name.
  `hostname` *`name`*
  `ip domain-name` *`name`*
- Step 4 – Generate an RSA key pair.
  `crypto key generate rsa` *`usage keys`*
- Step 5: Declare a CA.
  `crypto pki trustpoint` *`name`*

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco IOS Software CA Configuration Procedure (Continued)

Cisco.com

- Step 6 – Authenticate the CA
  `crypto pki authenticate` *`name`*
- Step 7 – Request a certificate for the router
  `crypto pki enroll` *`name`*
- Step 8 – Save the configuration
  `copy running-config startup-config`
- Step 9 – (Optional) Monitor and maintain CA interoperability
  `crypto pki trustpoint` *`name`*
- Step 10 – Verify the CA support configuration
  `show crypto pki certificates`
  `show crypto key mypubkey | pubkey-chain`

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 1 – (Optional) Manage NVRAM Memory Usage

Cisco.com

- Types of certificates stored on a router:
  - The identity certificate of the router
  - The root certificate of the CA
  - Root certificates obtained from CA servers
  - Two RA certificates, these are CA vendor-specific
- The number of CRLs stored on a router:
  - One, if the CA does not support an RA
  - Multiple, if the CA supports an RA

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 2 – Set the Router Time and Date

Cisco.com

router(config)#

```
clock timezone zone hours [minutes]
```

- Sets the router time zone and offset from UTC

```
RouterA(config)# clock timezone cst -6
```

router#

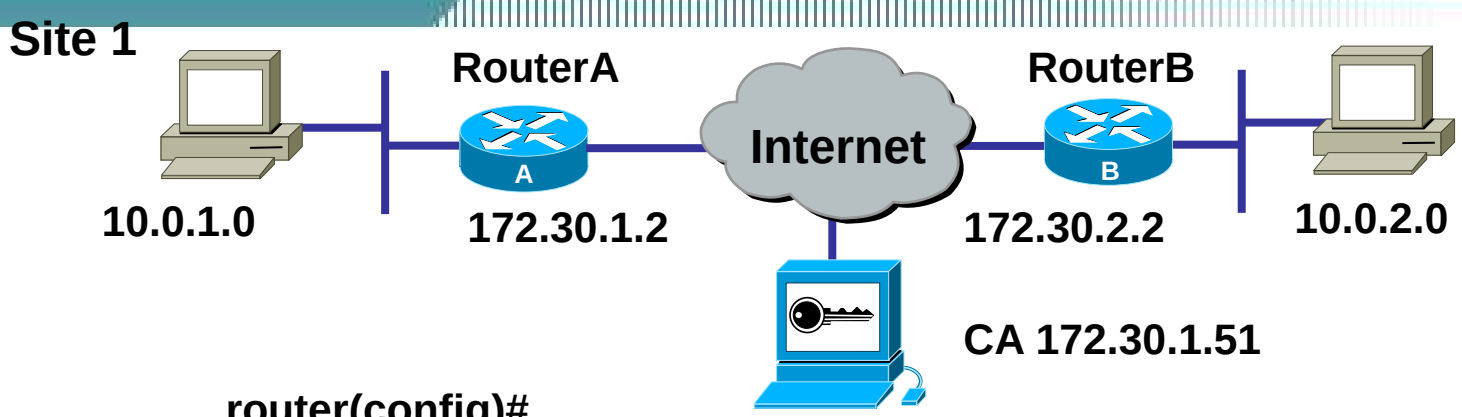
```
clock set hh:mm:ss day month year
clock set hh:mm:ss month day year
```

- Sets the router time and date

```
RouterA# clock set 23:59:59 17 February 2005
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 3 – Add a CA Server Entry to the Router Host Table



router(config)#

```
hostname name
```

- Specifies a unique name for the router

```
router(config)# hostname RouterA
```

router(config)#

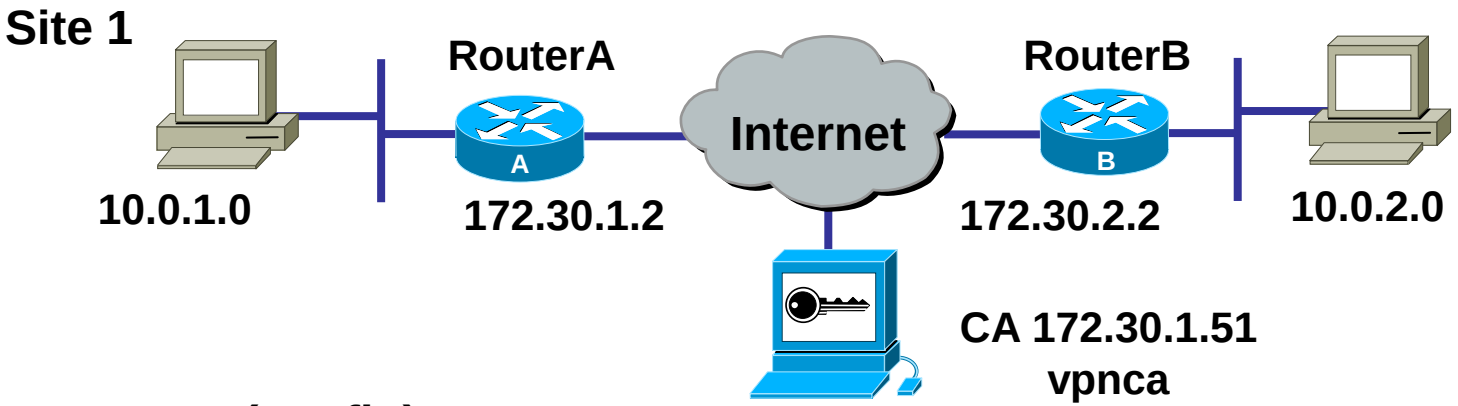
```
ip domain-name name
```

- Specifies a unique domain name for the router

```
RouterA(config)# ip domain-name xyz.com
```

ola.lundh@edu.falkenberg.se

Static Name-to-Address Mapping



router(config)#

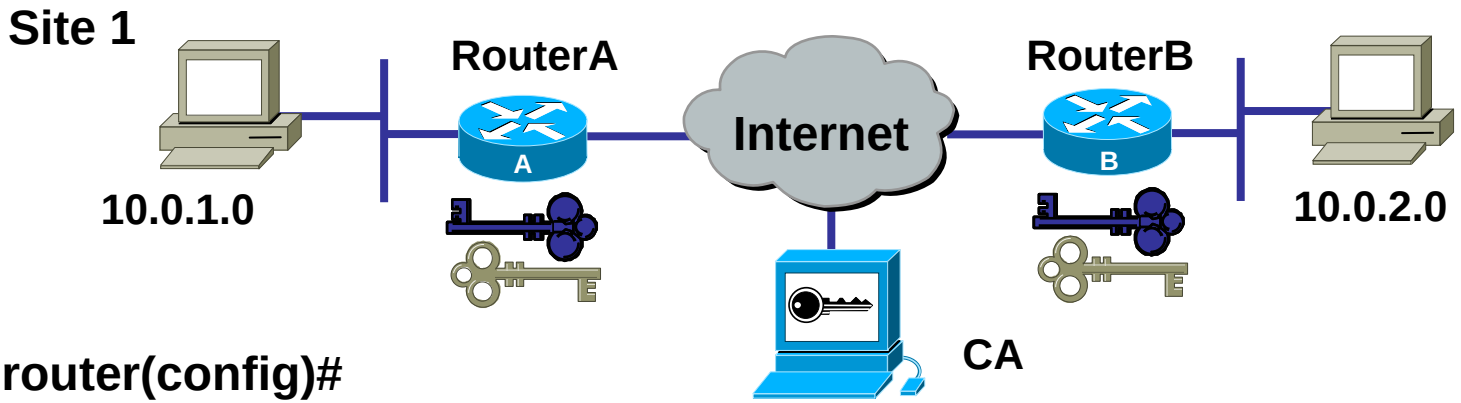
```
ip host name address1 [address2...addressN]
```

- **Defines a static hostname-to-address mapping for the CA server**
- **Step necessary if the domain name is not resolvable**

```
RouterA(config)# ip host vpnca 172.30.1.51
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 4 – Generate an RSA Key Pair




```
crypto key generate rsa [general-keys | usage-keys]
```

- **Using the keyword** usage-keys **generates two sets of RSA keys:**
  - **Use one key set for RSA signatures.**
  - **Use one key set for RSA encrypted nonces.**

```
RouterA(config)# crypto key generate rsa
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 4 – Generate RSA Keys – Example Output

Cisco.com

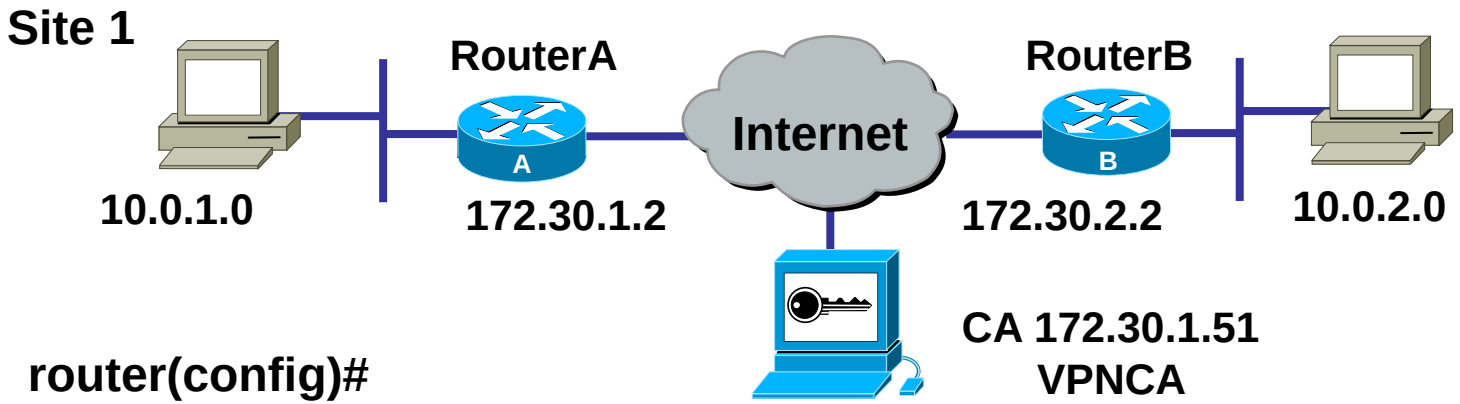
```
RouterA(config)# crypto key generate rsa
The name for the keys will be: router.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take a few
minutes.

How many bits in the modulus [512]: 512
Generating RSA keys ...
[OK]
```

```
RouterA# show crypto key mypubkey rsa
% Key pair was generated at: 23:58:59 UTC Dec 31 2000
Key name: RouterA.cisco.com
 Usage: General Purpose Key
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A9443B 62FDACFB
  CCDB8784 19AE1CD8 95B30953 1EDD30D1 380219D6 4636E015 4D7C6F33 4DC1F6E0
  C929A25E 521688A1 295907F4 E98BF920 6A81CE57 28A21116 E3020301 0001
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 5 – Declare a CA



router(config)#

```
crypto pki trustpoint name
```

- Specifies the desired CA server name
- Puts the administrator in the ca-trustpoint configuration mode

```
RouterA(config)# crypto pki trustpoint vpnca
RouterA(ca-trustpoint)#
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 5 – Commands Used to Declare a CA

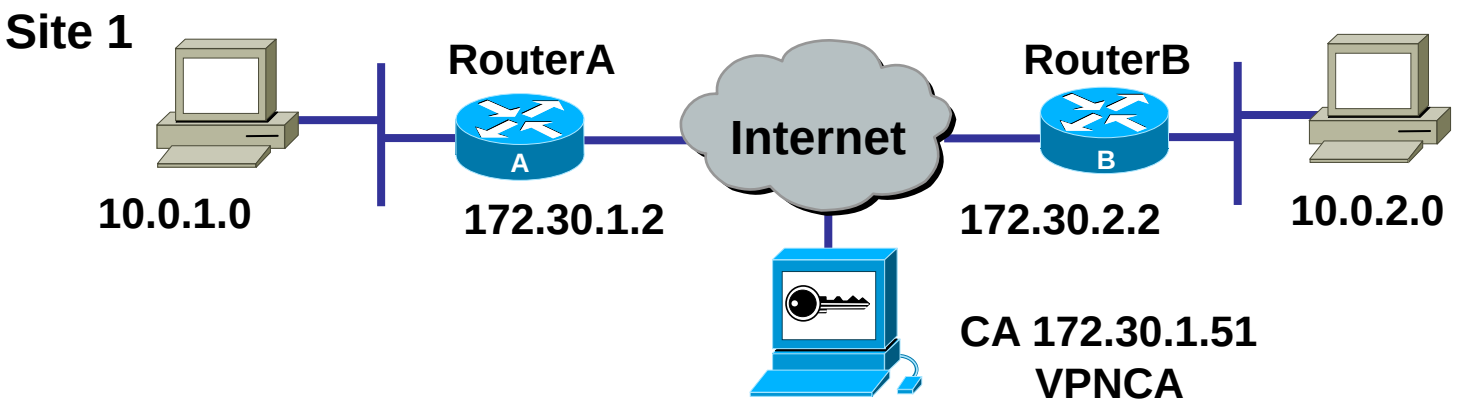
Cisco.com

```
RouterA(config)# crypto pki trustpoint vpnca
RouterA(ca-trustpoint)# ?
ca trustpoint configuration commands:
  crl           CRL option
  default       Set a command to its defaults
  enrollment    Enrollment parameters
  exit          Exit from certificate authority identity entry
                mode
  no            Negate a command or set its defaults
  query         Query parameters

RouterA(ca-trustpoint)# enrollment ?
  http-proxy    HTTP proxy server for enrollment
  mode          Mode supported by the Certicicate Authority
  retry         Polling parameters
  url           CA server enrollment URL
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 5 – Declare a CA

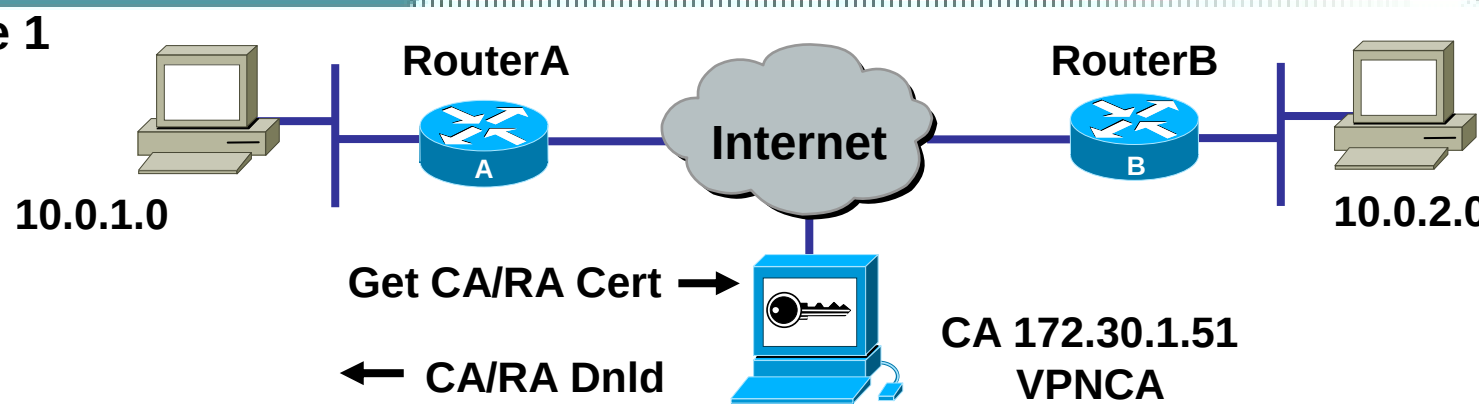



```
RouterA(config)# crypto pki trustpoint VPNCA
RouterA(ca-trustpoint)# enrollment url
      http://vpnca/certsrv/mscep/mscep.dll
RouterA(ca-trustpoint)# enrollment mode ra
RouterA(ca-trustpoint)# crl optional
```

- **Specifies the URL for the CA server**
- **Minimum configuration to declare a CA**

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 6 – Authenticate the CA



router(config)#

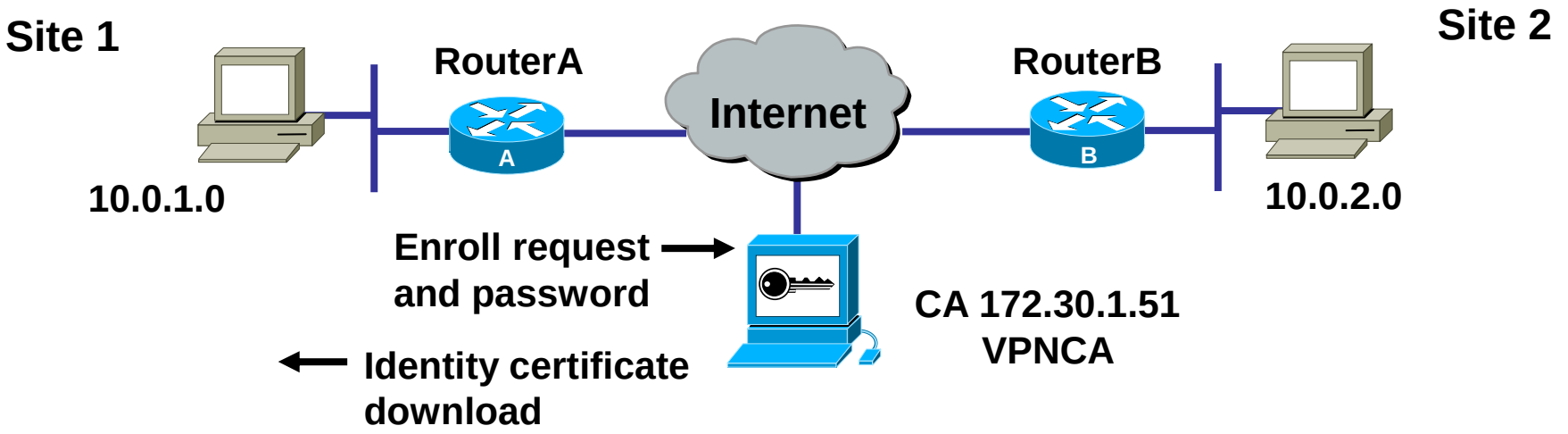
```
crypto pki authenticate name
```

– Manually authenticates the public key of the CA by contacting the CA administrator to compare the fingerprint of the CA certificate

```
RouterA(config)# crypto pki authenticate VPNCA
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 7 – Request a Certificate for the Router



router(config)#

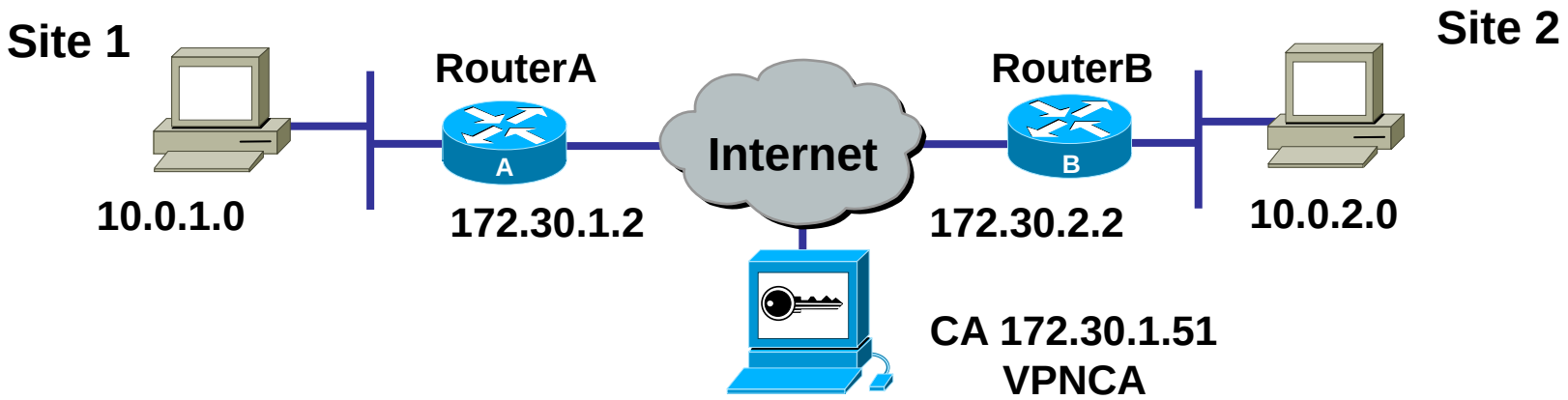
```
crypto pki enroll name
```

– Requests a signed identity certificate from the CA/RA

```
RouterA(config)# crypto pki enroll
VPNCA
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 8 – Save the Configuration

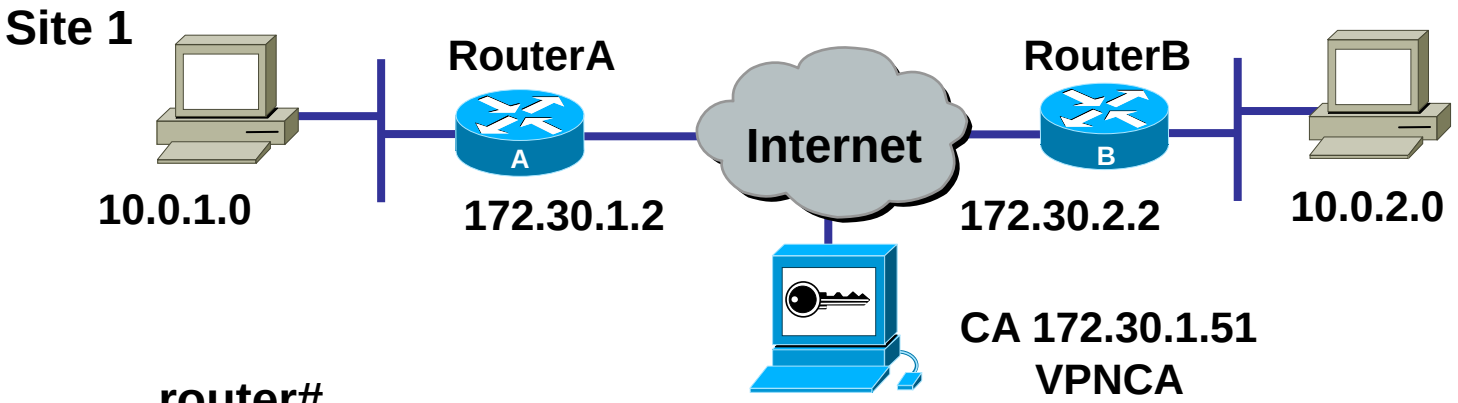



```
RouterA# copy running-config startup-config
```

- **Saves the running configuration of the router to NVRAM**

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Step 10 Verify the CA Support Configuration



router#

```
show crypto pki certificates
```

- View any configured CA or RA certificates

router#

```
show crypto key {mypubkey | pubkey-chain}
rsa
```

- View RSA keys for the router and other IPSec peers enrolled with a CA

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

CA Support Configuration Example

Cisco.com

```
RouterA# show running-config
!
hostname RouterA
!
ip domain-name cisco.com
!
crypto pki trustpoint VPNCA
 enrollment mode ra
 enrollment url http://vpnca:80
 query url ldap://vpnca
 crl optional
crypto pki certificate chain entrust
 certificate 37C6EAD6
  30820299 30820202 A0030201 02020437 C6EAD630 0D06092A
  864886F7 0D010105
  (certificates concatenated)
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems Networking Academy

Cisco.com

Module 5 – Configure Site-to-Site VPNs Using Digital Certificates

5.2 Configure an IOS Router Site-to-Site VPN Using Digital Certificates

CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

Configuration Tasks

- Prepare for ISAKMP and IPSec.
- Configure CA support.
- Configure ISAKMP.
- Configure IPSec.
- Test and verify IPSec.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Prepare for IPSec

Cisco.com

- Step 1 Plan for CA support
- Step 2 Determine the ISAKMP (IKE phase one) policy
- Step 3 Determine the IPSec (IKE phase two) policy
- Step 4 Check the current configuration
- Step 5 Ensure the network works without encryption
- Step 6 Ensure that access lists are compatible with IPSec

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

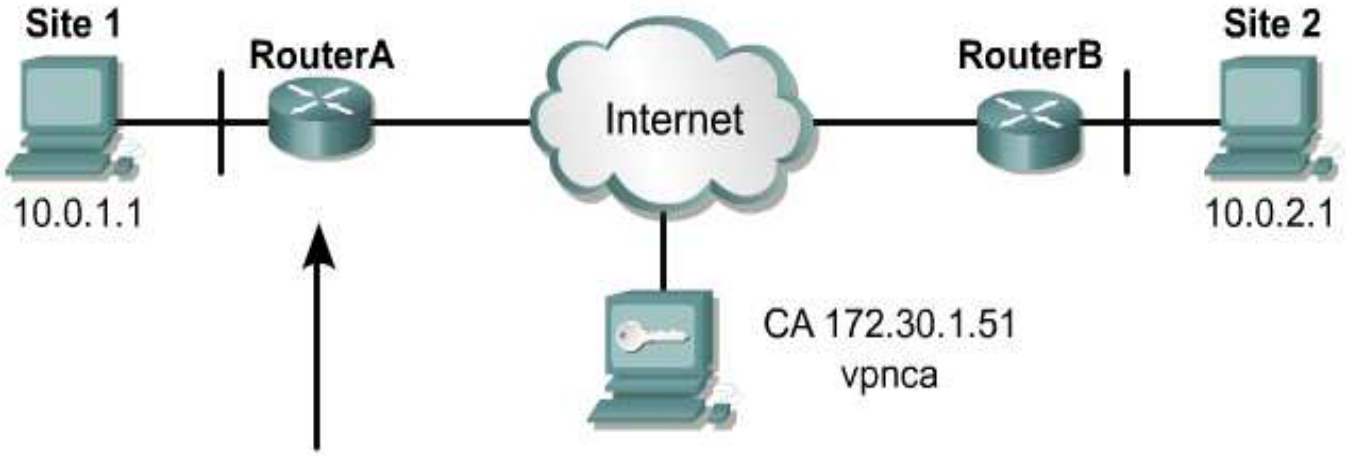
Configure the Router for CA Support

Cisco.com

- Step 1 Manage the non-volatile RAM (NVRAM) memory usage.
- Step 2 Set the router time and date.
- Step 3 Configure the router hostname and domain name.
- Step 4 Generate an RSA key pair
- Step 5 Declare a CA.
- Step 6 Authenticate the CA.
- Step 7 Request a certificate.
- Step 8 Save the configuration.
- Step 9 Monitor and maintain CA interoperability (Optional).
- Step 10 Verify the CA support configuration.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Create IKE Policies




```
RouterA(config)# crypto isakmp policy 110
RouterA(config-isakmp)# authentication rsa-sig
RouterA(config-isakmp)# encryption des
RouterA(config-isakmp)# group 1
RouterA(config-isakmp)# hash md5
RouterA(config-isakmp)# lifetime 86400
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Configure IPSec Encryption

- Configure transform set suites with the `crypto ipsec transform-set` command.
- Configure global IPSec security association lifetimes with the `crypto ipsec security-association lifetime` command.
- Configure crypto access lists with the `access-list` command.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Test and Verify IPSec

Cisco.com

- Display the configured transform sets using the `show crypto ipsec transform set` command.
- Display the current state of the IPSec SAs with the `show crypto ipsec sa` command.
- View the configured crypto maps with the `show crypto map` command.
- Debug IKE and IPSec traffic through the Cisco IOS with the `debug crypto ipseec` and `debug crypto isakmp` commands.
- Debug CA events through the Cisco IOS using the `debug crypto key-exchange` and `debug crypto pki` commands.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se