目 录

1 PKI配置

1.1 PKI简介

1.1.1 概述

PKI（Public Key Infrastructure，公钥基础设施）是一个利用公共密钥理论和技术来实现并提供信息安全服务的具有通用性的安全基础设施。

公共密钥体制也称为非对称密钥体制，是目前应用最广泛的一种加密体制，在这一体制中，它使用一个非对称的密钥对，分别是一个公开的加密密钥（公钥）和一个保密的解密密钥（私钥），用公钥加密的信息只能用私钥解密，反之亦然。由于公钥是公开的，需要在网上传送，故公钥的管理问题就是公共密钥体制所需要解决的关键问题。

目前，PKI 系统中引出的数字证书机制就是一个很好的解决方案。基于公共密钥技术的数字证书是一个用户的身份和他所持有的公钥的结合，它是使用 PKI 系统的用户建立安全通信的信任基础。

基于数字证书的 PKI 系统，能够为网络通信和网络交易，特别是电子政务和电子商务业务，透明地提供一整套安全服务，主要包括身份认证、保密、数据完整性和不可否认性。

目前，我司的 PKI 可为安全协议 IPsec（IP security，IP 安全）、SSL（Secure Sockets Layer，安全套接层）提供证书管理机制。

1.1.2 相关术语

1. 数字证书

数字证书是一个经 CA（Certificate Authority，证书机构）签名的、包含公开密钥及相关的用户身份信息的文件，它建立了用户身份信息与用户公钥的关联。CA 对数字证书的签名保证了证书的合法性和权威性。数字证书的格式遵循 ITU-T X.509 国际标准，目前最常用的为 X.509 V3 标准。一个数字证书中包含多个字段，包括证书签发者的名称、主体的公钥信息、CA 对证书的数字签名、证书的有效期等。

本手册中涉及两类证书：本地（local）证书和 CA（Certificate Authority）证书。本地证书是 CA 签发给用户的数字证书；CA 证书是 CA 自身的证书。若 PKI 系统中存在多个 CA，则会形成一个 CA 层次结构，最上层的 CA 是根 CA，它拥有一个 CA“自签名”的证书。

2. 证书废除列表（CRL，Certificate Revocation List）

由于用户姓名的改变、私钥泄漏或业务中止等原因，需要存在一种方法将现行的证书撤消，即撤消公开密钥及相关的用户身份信息的绑定关系。在 PKI 中，所使用的这种方法为证书废除列表。任何一个证书被废除以后，CA 就要发布 CRL 来声明该证书是无效的，并列出所有被废除的证书的序列号。CRL 提供了一种检验证书有效性的方式。

当一个 CRL 的撤消信息过多时会导致 CRL 的发布规模变得非常庞大，且随着 CRL 大小的增加，网络资源的使用性能也会随之下降。为了避免这种情况，允许一个 CA 的撤消信息通过多个 CRL 发布出来，并且使用 CRL 发布点来指出这些小 CRL 的位置。

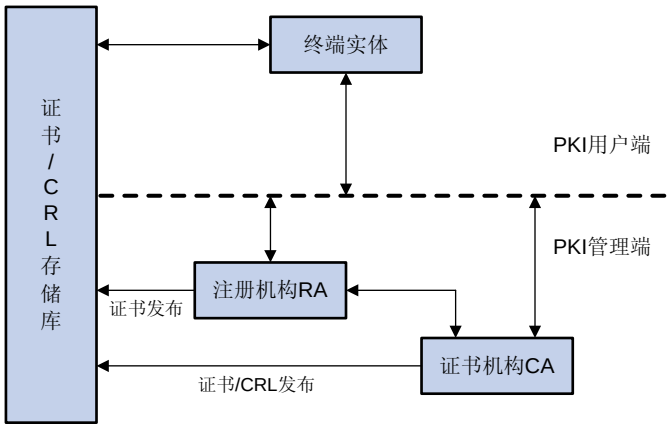
3. CA策略

CA 在受理证书请求、颁发证书、吊销证书和发布 CRL 时所采用的一套标准被称为 CA 策略。通常，CA 以一种叫做证书惯例声明（CPS，Certification Practice Statement）的文档发布其策略，CA 策略可以通过带外（如电话、磁盘、电子邮件等）或其他方式获取。由于不同的 CA 使用不同的方法验证公开密钥与实体之间的绑定，所以在选择信任的 CA 进行证书申请之前，必须理解 CA 策略，从而指导对实体进行相应的配置。

1.1.3 体系结构

一个PKI体系由终端实体、证书机构、注册机构和PKI存储库四类实体共同组成，如下 图 1-1。

图1-1 PKI 体系结构图



1. 终端实体

终端实体是 PKI 产品或服务的最终使用者，可以是个人、组织、设备（如路由器、交换机）或计算机中运行的进程。

2. 证书机构（CA，Certificate Authority）

CA 是 PKI 的信任基础，是一个用于签发并管理数字证书的可信实体。其作用包括：发放证书、规定证书的有效期和通过发布 CRL 确保必要时可以废除证书。

3. 注册机构（RA，Registration Authority）

RA 是 CA 的延伸，可作为 CA 的一部分，也可以独立。RA 功能包括个人身份审核、CRL 管理、密钥对产生和密钥对备份等。PKI 国际标准推荐由一个独立的 RA 来完成注册管理的任务，这样可以增强应用系统的安全性。

4. PKI存储库

PKI 存储库包括 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）服务器和普通数据库，用于对用户申请、证书、密钥、CRL 和日志等信息进行存储和管理，并提供一定的查询功能。

LDAP 提供了一种访问 PKI 存储库的方式，通过该协议来访问并管理 PKI 信息。LDAP 服务器负责将 RA 服务器传输过来的用户信息以及数字证书进行存储，并提供目录浏览服务。用户通过访问 LDAP 服务器获取自己和其他用户的数字证书。

1.1.4 主要应用

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。作为一种基础设施，PKI 的应用范围非常广泛，并且在不断发展之中，下面给出几个应用实例。

1. 虚拟专用网络（VPN，Virtual Private Network）

VPN 是一种构建在公用通信基础设施上的专用数据通信网络，利用网络层安全协议（如 IPsec）和建立在 PKI 上的加密与数字签名技术来获得机密性保护。

2. 安全电子邮件

电子邮件的安全也要求机密、完整、认证和不可否认，而这些都可以利用 PKI 技术来实现。目前发展很快的安全电子邮件协议 S/MIME(Secure/Multipurpose Internet Mail Extensions，安全/多用途 Internet 邮件扩充协议)，是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

3. Web安全

为了透明地解决 Web 的安全问题，在两个实体进行通信之前，先要建立 SSL（Secure Sockets Layer，安全套接字层）连接，以此实现对应用层透明的安全通信。SSL 协议允许在浏览器和服务器之间进行加密通信，并且利用 PKI 技术使用基于数字签名的方法对服务器和浏览器端进行身份验证。

1.1.5 PKI的工作过程

针对一个使用 PKI 的网络，配置 PKI 的目的就是为指定的实体向 CA 申请一个本地证书，并由设备对证书的有效性进行验证。下面是 PKI 的工作过程：

(1) 实体向 RA 提出证书申请；

(2) RA 审核实体身份，将实体身份信息和公开密钥以数字签名的方式发送给 CA；

(3) CA 验证数字签名，同意实体的申请，颁发证书；

(4) RA 接收 CA 返回的证书，发送到 LDAP 服务器以提供目录浏览服务，并通知实体证书发行成功；

(5) 实体获取证书，利用该证书可以与其它实体使用加密、数字签名进行安全通信；

(6) 实体希望撤消自己的证书时，向 CA 提交申请。CA 批准实体撤消证书，并更新 CRL，发布到 LDAP 服务器。

1.2 PKI配置任务简介

表1-1 PKI 配置任务简介

配置任务		说明	详细配置
配置实体 DN		必选	1.3
配置 PKI 域		必选	1.4
PKI 证书申请	自动申请证书	二者必选其一	1.5.1
	手工申请证书		1.5.2
手工获取证书		可选	1.6

配置任务	说明	详细配置
配置 PKI 证书验证	可选	1.7
销毁本地 RSA 或 DSA 密钥对	可选	1.8
删除证书	可选	1.9
配置证书属性的访问控制策略	可选	1.10

1.3 配置实体DN

一份证书是一个公开密钥与一个身份的绑定，而身份必须与一个特定的 PKI 实体相关联。实体 DN（Distinguished Name，可识别名称）的参数是实体的身份信息，CA 根据实体提供的身份信息来唯一标识证书申请者。

实体 DN 的参数包括：

- 实体通用名
- 实体所属国家代码，用标准的两字符代码表示。例如，“CN”是中国的合法国家代码，“US”是美国的合法国家代码
- 实体 FQDN（Fully Qualified Domain Name，合格域名），是实体在网络中的唯一标识，由一个主机名和域名组成，可被解析为 IP 地址。例如，www 是一个主机名，whatever.com 是一个域名，则 www.whatever.com 就是一个 FQDN。
- 实体 IP 地址
- 实体所在地理区域名称
- 实体所属组织名称
- 实体所属部门名称
- 实体所属州省

说明

实体 DN 的配置必须与 CA 证书颁发策略相匹配，以确认实体 DN 的配置任务，如哪些实体参数为必选配置，哪些为可选配置。申请者的身份信息必须符合 CA 证书颁发策略，否则证书申请可能会失败。

表1-2 配置实体 DN

操作	命令	说明
进入系统视图	**system-view**	-
创建一个实体，并进入该实体视图	**pki entity** *entity-name*	必选 缺省情况下，无实体存在
配置实体通用名	**common-name** *name*	可选 缺省情况下，未配置实体的通用名

操作	命令	说明
配置实体所属国家代码	**country** *country-code-str*	可选 缺省情况下，未配置实体所属国家代码
配置实体 FQDN	**fqdn** *name-str*	可选 缺省情况下，未配置实体 FQDN
配置实体 IP 地址	**ip** *ip-address*	可选 缺省情况下，未配置实体 IP 地址
配置实体所在地理区域名称	**locality** *locality-name*	可选 缺省情况下，未配置实体所在地理区域
配置实体所属组织名称	**organization** *org-name*	可选 缺省情况下，未配置实体所属组织
配置实体所属部门名称	**organization-unit** *org-unit-name*	可选 缺省情况下，未配置实体所属部门
配置实体所属州省	**state** *state-name*	可选 缺省情况下，未配置实体所属州省

说明

- 目前一台设备上最多可以创建两个实体。
- Windows 2000 CA 服务器对证书申请的数据长度有一定的限制。实体 DN 配置项超过一定数据长度时，申请证书没有回应。

1.4 配置PKI域

实体在进行 PKI 证书申请操作之前需要配置一些注册信息来配合完成申请的过程。这些信息的集合就是一个实体的 PKI 域。

PKI 域是一个本地概念，因此创建 PKI 域的目的是便于其它应用引用 PKI 的配置，比如 IKE、SSL 等。一个设备上配置的 PKI 域对 CA 和其它设备是不可见的，每一个 PKI 域有单独的域参数配置信息。

PKI 域中包括以下参数：

- 信任的 CA 名称

在申请证书时，是通过一个可信实体认证机构，来完成实体证书的注册颁发，因此必须指定一个信任的 CA 名称。

- 实体名称

向 CA 发送证书申请请求时，必须指定所使用的实体名，以向 CA 表明自己的身份。

- 证书申请的注册机构

证书申请的受理一般由一个独立的注册机构（即 RA）来承担，它接收用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书，而只是对用

户进行资格审查。有时 PKI 把注册管理的职能交给 CA 来完成，而不设立独立运行的 RA，但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。PKI 推荐独立使用 RA 作为注册审理机构。

- 注册服务器的 URL

证书申请之前必须指定注册服务器的 URL，随后实体可通过简单证书注册协议（SCEP，Simple Certification Enrollment Protocol）向该服务器提出证书申请，SCEP 是专门用于与认证机构进行通信的协议。

- 证书申请状态查询的周期和次数

实体在发送证书申请后，如果 CA 采用手工验证申请，证书的发布会需要很长时间。在此期间，客户端需要定期发送状态查询，以便在证书签发后能及时获取到证书。客户端可以配置证书申请状态的查询周期和次数。

- LDAP 服务器 IP 地址

在 PKI 系统中，用户的证书和 CRL 信息的存储是一个非常核心的问题。一般采用 LDAP 服务器来存储证书和 CRL，这时就需要指定 LDAP 服务器的位置。

- 验证根证书时使用的指纹

当设备从 CA 获得根证书时，需要验证 CA 根证书的指纹，即根证书内容的散列值，该值对于每一个证书都是唯一的。如果 CA 根证书的指纹与在 PKI 域中配置的指纹不同，则设备将拒绝接收根证书。

表1-3 配置 PKI 域

配置任务	命令	说明
进入系统视图	**system-view**	-
创建一个 PKI 域，并进入 PKI 域视图	**pki domain** *domain-name*	必选
配置信任的 CA 名称	**ca identifier** *name*	必选 缺省情况下，未配置信任的 CA 名称
指定实体名称	**certificate request entity** *entity-name*	必选 缺省情况下，未指定实体名称 指定的实体名称必须已创建
配置证书申请的注册受理机构	**certificate request from** { **ca** | **ra** }	必选 缺省情况下，未指定证书申请的注册受理机构
配置注册服务器 URL	**certificate request url** *url-string*	必选 缺省情况下，未指定注册服务器 URL
配置证书申请状态查询的周期和次数	**certificate request polling** { **count** *count* | **interval** *minutes* }	可选 缺省情况下，证书申请状态查询周期为 20 分钟，每一个周期内查询 50 次
配置 LDAP 服务器	**ldap-server ip** *ip-address* [**port** *port-number*] [**version** *version-number*]	可选 缺省情况下，未指定 LDAP 服务器

配置任务	命令	说明
配置验证根证书时使用的指纹	**root-certificate fingerprint** { **md5** | **sha1** } *string*	当证书申请方式为自动方式时，此配置必选；当证书申请方式为手工方式时，此配置可选，若不配置，需要用户自行验证根证书指纹 缺省情况下，未指定验证根证书时使用的指纹

说明

- 目前一台设备只支持同时创建两个 PKI 域。
- CA 的名称只是在获取 CA 证书时使用，申请本地证书时不会用到。
- 目前，注册服务器 URL 的配置不支持域名解析。

1.5 PKI证书申请

证书申请就是实体向 CA 自我介绍的过程。实体向 CA 提供身份信息，以及相应的公开密钥，这些信息将成为颁发给该实体证书的主要组成部分。实体向 CA 提出证书申请，有离线和在线两种方式。离线申请方式下，CA 允许申请方通过带外方式（如电话、磁盘、电子邮件等）向 CA 提供申请信息。

在线证书申请有手工发起和自动发起两种方式。

1.5.1 自动申请证书

配置证书申请方式为自动方式后，当有应用协议与 PKI 联动时，如果应用协议中的实体无本地证书（例如，IKE 协商采用数字签名方法进行身份认证，但在协商过程中没有发现本地证书），则实体自动通过 SCEP 协议向 CA 发起证书申请。

表1-4 自动申请证书

操作	命令	说明
进入系统视图	**system-view**	-
进入 PKI 域视图	**pki domain** *domain-name*	-
配置证书申请为自动方式	**certificate request mode auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*] *	必选 缺省情况下，证书申请为手工方式

说明

在自动申请到的证书即将过期时以及正式过期后，系统不会重新申请新的证书，这种情况下，可能会由于证书过期造成应用业务的中断，因此建议用户手工申请证书。

1.5.2 手工申请证书

配置证书申请方式为手工方式后，需要手工完成获取 CA 证书、生成密钥对、申请本地证书的工作。

获取 CA 证书的目的是用来验证本地证书的真实性和合法性。

密钥对的产生是证书申请过程中重要的一步。申请过程使用了一对主机密钥：私钥和公钥。私钥由用户保留，公钥和其他信息则交由 CA 中心进行签名，从而产生证书。

有关 RSA 和 DSA 密钥对的具体配置请参见“安全配置指导”中的“公钥管理”。

表1-5 手工申请证书

操作	命令	说明
进入系统视图	**system-view**	-
进入 PKI 域视图	**pki domain** *domain-name*	-
配置证书申请为手工方式	**certificate request mode manual**	可选 缺省情况下，证书申请为手工方式
退回系统视图	**quit**	-
手工获取 CA 证书	请参见 1.6	必选
生成本地 RSA 或 DSA 密钥对	**public-key local create** { **dsa** | **rsa** }	必选
手工申请本地证书	**pki request-certificate domain** *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]	必选

说明

- 若本地证书已存在，为保证密钥对与现存证书的一致性，不应执行创建密钥对命令，必须在删除本地证书后再执行 **public-key local create** 命令生成新的密钥对。有关 **public-key local create** 命令的详细介绍，请参见“安全命令参考”中的“公钥管理”。
- 创建的新密钥对将覆盖旧密钥对。若本地已有 RSA 或 DSA 密钥对，执行 **public-key local create** 命令时，系统会提示是否替换原有密钥对。
- 如果本地证书已存在，则不允许再执行证书申请操作，以避免因相关配置的修改使得证书与注册信息不匹配。若想重新申请，请先使用 **pki delete-certificate** 命令删除存储于本地的 CA 证书与本地证书，然后再执行 **pki request-certificate domain** 命令。
- 当无法通过 SCEP 协议向 CA 在线申请证书时，可以首先通过执行指定参数 **pkcs10** 的命令 **pki request-certificate domain** 打印出本地的证书申请信息，或者通过执行指定 **pkcs10 filename** *filename* 参数的该命令将证书申请信息直接保存到本地的指定文件中，然后再通过带外方式将这些本地证书申请信息发送给 CA 进行证书申请。
- 证书申请之前必须保证实体时钟与 CA 的时钟同步，否则申请证书的有效期会出现异常。
- **pki request-certificate domain** 配置不能被保存在配置文件中。

1.6 手工获取证书

用户通过此配置可以将已存在的 CA 证书、本地证书或者外部实体证书获取至本地。获取证书有两种方式：离线方式和在线方式。离线方式下获取证书需要通过带外方式（如 FTP、磁盘、电子邮件等）取得证书，然后将其导入至本地。

获取证书的目的有两个：

- 将 CA 签发的与实体所在安全域有关的证书存放到本地，以提高证书的查询效率，减少向 PKI 证书存储库查询的次数。
- 为证书的验证做好准备。

在线获取本地证书之前必须完成 LDAP 服务器的配置。

表1-6 手工获取证书

操作		命令	说明
进入系统视图		**system-view**	-
手工获取证书	在线方式	**pki retrieval-certificate** { **ca** | **local** } **domain** *domain-name*	二者必选其一
	离线方式导入证书	**pki import-certificate** { **ca** | **local** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]	

注意

- 如果本地已有 CA 证书存在，则不允许执行手工获取 CA 证书的操作，避免因相关配置的修改使得证书与注册信息不匹配。若想重新获取，请先使用 **pki delete-certificate** 命令删除 CA 证书与本地证书后，再执行此命令。
- **pki retrieval-certificate** 配置不能被保存在配置文件中。
- 为保证设备上已申请的证书可用，请确保设备当前系统时间处于证书的有效期范围之内。

1.7 配置PKI证书验证

在使用每一个证书之前，必须对证书进行验证。证书验证包括对签发时间、签发者信息以及证书的有效性几方面进行验证。证书验证的核心是检查 CA 在证书上的签名，并确定证书仍在有效期内，而且未被废除，因此在进行证书验证操作之前必须首先获取 CA 证书。

配置证书验证时可以设置是否必须进行 CRL 检查。

- 如果配置为使能 CRL 检查，则检验证书的有效性，必须通过 CRL 判断。因此，在进行证书有效性验证之前，除了获取 CA 证书还必须获取 CRL 并下载至本地；
- 如果配置为不使能 CRL 检查，则仅需要获取 CA 证书来判断证书的有效性。

1.7.1 配置使能CRL检查的证书验证

表1-7 配置使能 CRL 检查的证书验证

操作	命令	说明
进入系统视图	**system-view**	-
进入 PKI 域视图	**pki domain** *domain-name*	-
配置 CRL 发布点的 URL	**crl url** *url-string*	可选 缺省情况下，未指定 CRL 发布点的 URL
配置 CRL 的更新周期	**crl update-period** *hours*	可选 缺省情况下，根据 CRL 文件中的下次更新域进行更新
使能 CRL 检查	**crl check enable**	可选 缺省情况下，CRL 检查处于开启状态
退回系统视图	**quit**	-
获取 CA 证书	请参见 1.6	必选
获取 CRL 并下载至本地	**pki retrieval-crl domain** *domain-name*	必选
检验证书的有效性	**pki validate-certificate** { **ca** | **local** } **domain** *domain-name*	必选

说明

- CRL 的更新周期是指本地从 CRL 存储服务器下载 CRL 的时间间隔。手工配置的 CRL 更新周期将优先于 CRL 文件中指定的更新时间。
- **pki retrieval-crl domain** 命令不能被保存在配置文件中。
- 目前，CRL 发布点 URL 的配置不支持域名解析。

1.7.2 配置不使能CRL检查的PKI证书验证

表1-8 配置不使能 CRL 检查的 PKI 证书验证

操作	命令	说明
进入系统视图	**system-view**	-
进入 PKI 域视图	**pki domain** *domain-name*	-
禁止 CRL 检查	**crl check disable**	必选 缺省情况下，CRL 检查处于开启状态
退回系统视图	**quit**	-

操作	命令	说明
获取 CA 证书	请参见 1.6	必选
检验证书的有效性	**pki validate-certificate** { **ca** | **local** } **domain** *domain-name*	必选

1.8 销毁本地RSA或DSA密钥对

由 CA 颁发的证书都会设置有效期，证书生命周期的长短由签发证书的 CA 中心来确定。当用户的私钥被泄漏或证书的有效期快到时，用户应该删除旧的密钥对，产生新的密钥对，重新申请新的证书。通过此配置用户可以销毁本地 RSA 或 DSA 密钥对。

表1-9 销毁本地 RSA 密钥对

操作	命令	说明
进入系统视图	**system-view**	-
销毁本地 RSA 或 DSA 密钥对	**public-key local destroy** { **dsa** | **rsa** }	必选

说明

命令 **public-key local destroy** 的详细介绍可参考“安全命令参考”中的“公钥管理”。

1.9 删除证书

证书过期或希望重新申请证书，可以通过此配置删除一个已经存在的本地证书或 CA 证书。

表1-10 配置删除证书

操作	命令	说明
进入系统视图	**system-view**	-
配置删除证书	**pki delete-certificate** { **ca** | **local** } **domain** *domain-name*	必选

1.10 配置证书属性的访问控制策略

通过配置证书属性的访问控制策略，可以对用户的访问权限进行进一步的控制，保证了与之通信的服务器的安全性。

表1-11 配置证书属性的访问控制策略

操作	命令	说明
进入系统视图	**system-view**	-
创建证书属性组，并进入证书属性组视图	**pki certificate attribute-group** *group-name*	必选 缺省情况下，不存在证书属性组
配置证书颁发者名、证书主题名及备用主题名的属性规则	**attribute** *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ**} *attribute-value*	可选 缺省情况下，对证书颁发者名、证书主题名及备用主题名没有限制
退回系统视图	**quit**	-
创建证书属性访问控制策略，并进入证书属性访问控制策略视图	**pki certificate access-control-policy** *policy-name*	必选 缺省情况下，不存在证书属性访问控制策略
配置证书属性控制规则	**rule** [*id*] { **deny** | **permit** } *group-name*	必选 缺省情况下，不存在证书属性控制规则 *group-name* 必须是已存在的证书属性组的名称

1.11 PKI显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 PKI 的运行情况，通过查看显示信息验证配置的效果。

表1-12 PKI 显示和维护

操作	命令
显示证书内容或证书申请状态	**display pki certificate** { { **ca** | **local** } **domain** *domain-name* | **request-status** } [| { **begin** | **exclude** | **include** } *regular-expression*]
显示 CRL 内容	**display pki crl domain** *domain-name* [| { **begin** | **exclude** | **include** } *regular-expression*]
显示证书属性组的信息	**display pki certificate attribute-group** { *group-name* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]
显示证书属性访问控制策略的信息	**display pki certificate access-control-policy** { *policy-name* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]

1.12 PKI典型配置举例

注意

- 当采用 Windows Server 作为 CA 时，需要安装 SCEP 插件。此时，配置 PKI domain 时，需要使用 **certificate request from ra** 命令指定实体从 RA 注册申请证书。
- 当采用 RSA Keon 软件时，不需要安装 SCEP 插件。此时，配置 PKI domain 时，需要使用 **certificate request from ca** 命令指定实体从 CA 注册申请证书。

1.12.1 PKI实体向CA申请证书（采用RSA Keon CA服务器）

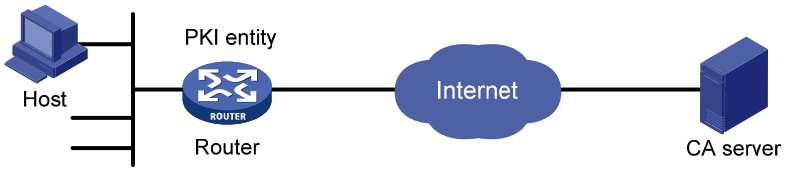
1. 组网需求

在作为 PKI 实体的设备 Router 上进行相关配置，实现以下需求：

- 设备向 CA 服务器申请本地证书
- 获取 CRL 为证书验证做准备

2. 组网图

图1-2 PKI 实体向 CA 申请证书组网图



3. 配置步骤

(1) 配置 CA 服务器

- 创建 CA 服务器 myca

在本例中，CA 服务器上首先需要进行基本属性 Nickname 和 Subject DN 的配置。其它属性选择默认值。其中，Nickname 为可信任的 CA 名称，Subject DN 为 CA 的 DN 属性，包括 CN、OU、O 和 C。

- 配置扩展属性

基本属性配置完毕之后，还需要在生成的 CA 服务器管理页面上对“Jurisdiction Configuration”进行配置，主要内容包括：根据需要选择合适的扩展选项；启动自动颁发证书功能；添加可以自动颁发证书的地址范围。

- 配置 CRL 发布

CA 服务器的基本配置完成之后，需要进行 CRL 的相关配置。

本例中选择 CRL 的发布方式为 HTTP，自动生成 CRL 发布点的 URL 为 http://4.4.4.133:447/myca.crl。

以上配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书和获取 CRL。

(2) 配置 Router

- 配置实体命名空间

配置实体名称为 aaa，通用名为 router。

```
<Router> system-view
[Router] pki entity aaa
[Router-pki-entity-aaa] common-name router
[Router-pki-entity-aaa] quit
```

- 配置 PKI 域参数

创建并进入 PKI 域 torsa。

```
[Router] pki domain torsa
```

配置可信任的 CA 名称为 myca。

```
[Router-pki-domain-torsa] ca identifier myca
```

配置注册服务器 URL，格式为 http://host:port/Issuing Jurisdiction ID。其中的 Issuing Jurisdiction ID 为 CA 服务器上生成的 16 进制字符串。

```
[Router-pki-domain-torsa] certificate request url
http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

配置证书申请的注册受理机构为 CA。

```
[Router-pki-domain-torsa] certificate request from ca
```

指定实体名称为 aaa。

```
[Router-pki-domain-torsa] certificate request entity aaa
```

配置 CRL 发布点位置。

```
[Router-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl
[Router-pki-domain-torsa] quit
```

- 用 RSA 算法生成本地密钥对

```
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
```

- 证书申请

获取 CA 证书并下载至本地。

```
[Router] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while......
The trusted CA's finger print is:
    MD5  fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB
    SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8
```

```
Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment......
CA certificates retrieval success.
```

获取 CRL 并下载至本地。

```
[Router] pki retrieval-crl domain torsa
Connecting to server for retrieving CRL. Please wait a while.....
CRL retrieval success!
```

手工申请本地证书。

```
[Router] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait......
[Router]
Enrolling the local certificate,please wait a while......
Certificate request Successfully!
Saving the local certificate to device......
Done!
```

4. 验证配置结果

通过以下显示命令可以查看获取的本地证书信息。

```
[Router] display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9A96A48F 9A509FD7 05FFF4DF 104AD094
        Issuer:
            C=cn
            O=org
            OU=test
            CN=myca
        Validity
            Not Before: Jan  8 09:26:53 2007 GMT
            Not After : Jan  8 09:26:53 2008 GMT
        Subject:
            CN=router
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00D67D50 41046F6A 43610335 CA6C4B11
                    F8F89138 E4E905BD 43953BA2 623A54C0
                    EA3CB6E0 B04649CE C9CDDD38 34015970
                    981E96D9 FF4F7B73 A5155649 E583AC61
                    D3A5C849 CBDE350D 2A1926B7 0AE5EF5E
                    D1D8B08A DBF16205 7C2A4011 05F11094
                    73EB0549 A65D9E74 0F2953F2 D4F0042F
                    19103439 3D4F9359 88FB59F3 8D4B2F6C
                    2B
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:
            URI:http://4.4.4.133:447/myca.crl
```

关于获取的 CA 证书及 CRL 文件的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令 **display pki certificate ca domain** 和 **display pki crl domain**。

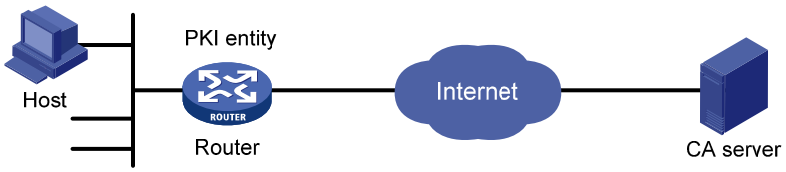
1.12.2 PKI实体向CA申请证书（采用Windows 2003 server CA服务器）

1. 组网需求

配置 PKI 实体 Router 向 CA 服务器申请本地证书。

2. 组网图

图1-3 PKI 实体向 CA 申请证书组网图



3. 配置步骤

(1) 配置 CA 服务器

- 安装证书服务器组件

打开[控制面板]/[添加/删除程序]，选择[添加/删除 Windows 组件]中的“证书服务”进行安装。

- 安装 SCEP 插件

由于 Windows 2003 server 作为 CA 服务器时，缺省情况下不支持 SCEP，所以需要安装 SCEP 插件，才能使设备具备证书自动注册、获取等功能。插件安装完毕后，弹出提示框，提示框中的 URL 地址即为设备上配置的注册服务器地址。

- 修改证书服务的属性

完成上述配置后，打开[控制面板/管理工具]中的[证书颁发机构]，如果安装成功，在[颁发的证书]中将存在两个 CA 颁发给 RA 的证书。选择[CA server 属性]中的“策略模块”的属性为“如果可以的话，按照证书模板中的设置。否则，将自动颁发证书(F)。”

- 修改 IIS 服务的属性

打开[控制面板/管理工具]中的[Internet 信息服务(IIS)管理器]，将[默认网站 属性]中“主目录”的本地路径修改为证书服务保存的路径。另外，为了避免与已有的服务冲突，建议修改默认网站的 TCP 端口号为未使用的端口号。

以上配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书。

(2) 配置 Router

- 配置实体命名空间

配置实体名称为 aaa，通用名为 router。

```
<Router> system-view
[Router] pki entity aaa
```

```
[Router-pki-entity-aaa] common-name router
[Router-pki-entity-aaa] quit
```

- 配置 PKI 域参数

创建并进入 PKI 域 torsa。

```
[Router] pki domain torsa
```

配置可信任的 CA 名称为 myca。

```
[Router-pki-domain-torsa] ca identifier myca
```

配置注册服务器 URL，格式为 http://host:port/certsrv/mscep/mscep.dll。其中，host:port 为 CA 服务器的主机地址和端口号。

```
[Router-pki-domain-torsa] certificate request url
http://4.4.4.1:8080/certsrv/mscep/mscep.dll
```

配置证书申请的注册受理机构为 RA。

```
[Router-pki-domain-torsa] certificate request from ra
```

指定实体名称为 aaa。

```
[Router-pki-domain-torsa] certificate request entity aaa
```

- 用 RSA 算法生成本地密钥对

```
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
```

- 证书申请

获取 CA 证书并下载至本地。

```
[Router] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while......
The trusted CA's finger print is:
    MD5  fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB
    SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment......
CA certificates retrieval success.
```

手工申请本地证书。

```
[Router] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait......
[Router]
Enrolling the local certificate,please wait a while......
Certificate request Successfully!
```

```
Saving the local certificate to device......
Done!
```

4. 验证配置结果

通过以下显示命令可以查看获取的本地证书信息。

```
[Router] display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48FA0FD9 00000000 000C
        Issuer:
            CN=myca
        Validity
            Not Before: Nov 21 12:32:16 2007 GMT
            Not After : Nov 21 12:42:16 2008 GMT
        Subject:
            CN=router
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00A6637A 8CDEA1AC B2E04A59 F7F6A9FE
                    5AEE52AE 14A392E4 E0E5D458 0D341113
                    0BF91E57 FA8C67AC 6CE8FEBB 5570178B
                    10242FDD D3947F5E 2DA70BD9 1FAF07E5
                    1D167CE1 FC20394F 476F5C08 C5067DF9
                    CB4D05E6 55DC11B6 9F4C014D EA600306
                    81D403CF 2D93BC5A 8AF3224D 1125E439
                    78ECEFE1 7FA9AE7B 877B50B8 3280509F
                    6B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
            B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1
            X509v3 Authority Key Identifier:
            keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

            X509v3 CRL Distribution Points:
            URI:http://l00192b/CertEnroll/CA%20server.crl
            URI:file://\\l00192b\CertEnroll\CA server.crl

            Authority Information Access:
            CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt
            CA Issuers - URI:file://\\l00192b\CertEnroll\l00192b_CA server.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
```

关于获取的 CA 证书的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令**display pki certificate ca domain**。

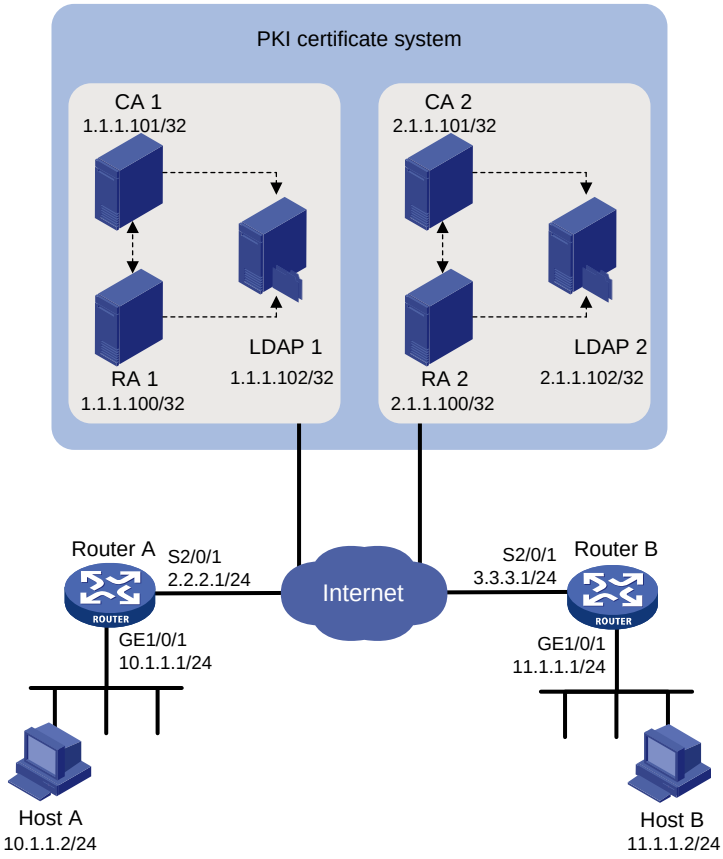
1.12.3 使用PKI证书体系的RSA证书签名方法进行IKE协商认证

1. 组网需求

- 在 Router A 和 Router B 之间建立一个 IPsec 安全隧道对子网 10.1.1.0/24 上的主机 A 与子网 11.1.1.0/24 上的主机 B 之间的数据流进行安全保护。
- 在 Router A 和 Router B 之间使用 IKE 自动协商建立安全通信，IKE 认证策略采用 PKI 证书体系的 RSA 证书签名方法进行身份认证。
- 图 1-4中Router A和Router B使用不同的CA（可以相同，根据实际情况确定）。

2. 组网图

图1-4 PKI 进行 IKE 协商认证的组网图



3. 配置步骤

(1) 配置 Router A

配置实体命名空间。

```
<RouterA> system-view
[RouterA] pki entity en
[RouterA-pki-entity-en] ip 2.2.2.1
[RouterA-pki-entity-en] common-name routera
[RouterA-pki-entity-en] quit
```

配置 PKI 域参数。（证书申请的注册机构服务器的 URL 根据所使用的 CA 服务器的不同而有所不同，这里的配置只作为示例，请根据具体情况配置。）

```
[RouterA] pki domain 1
[RouterA-pki-domain-1] ca identifier CA1
[RouterA-pki-domain-1] certificate request url http://1.1.1.100/certsrv/mscep/mscep.dll
[RouterA-pki-domain-1] certificate request entity en
[RouterA-pki-domain-1] ldap-server ip 1.1.1.102
```

配置通过 RA 注册申请证书。

```
[RouterA-pki-domain-1] certificate request from ra
```

配置 CRL 发布点位置（若禁止 CRL 检查，则无需配置）。

```
[RouterA-pki-domain-1] crl url ldap://1.1.1.102
[RouterA-pki-domain-1] quit
```

用 RSA 算法生成本地的密钥对。

```
[RouterA] public-key local create rsa
```

证书申请。

```
[RouterA] pki retrieval-certificate ca domain 1
[RouterA] pki retrieval-crl domain 1
[RouterA] pki request-certificate domain 1
```

配置 IKE 提议 1，使用数字签名（rsa-signature）方法为身份认证策略。

```
[RouterA] ike proposal 1
[RouterA-ike-proposal-1] authentication-method rsa-signature
[RouterA-ike-proposal-1] quit
```

在 IKE 对等体中引用 PKI 域的配置。

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] certificate domain 1
```

(2) 配置 Router B

配置实体命名空间。

```
<RouterB> system-view
[RouterB] pki entity en
[RouterB-pki-entity-en] ip 3.3.3.1
[RouterB-pki-entity-en] common-name routerb
[RouterB-pki-entity-en] quit
```

配置 PKI 域参数。（证书申请的注册机构服务器的 URL 根据所使用的 CA 服务器的不同而有所不同，这里的配置只作为示例，请根据具体情况配置。）

```
[RouterB] pki domain 1
[RouterB-pki-domain-1] ca identifier CA2
[RouterB-pki-domain-1] certificate request url http://2.1.1.100/certsrv/mscep/mscep.dll
[RouterB-pki-domain-1] certificate request entity en
[RouterB-pki-domain-1] ldap-server ip 2.1.1.102
```

配置通过 RA 注册申请证书。

```
[RouterB-pki-domain-1] certificate request from ra
```

配置 CRL 发布点（若禁止 CRL 检查，则无需配置）。

```
[RouterB-pki-domain-1] crl url ldap://2.1.1.102
[RouterB-pki-domain-1] quit
```

用 RSA 算法生成本地的密钥对。

```
[RouterB] public-key local create rsa
```

证书申请。

```
[RouterB] pki retrieval-certificate ca domain 1
[RouterB] pki retrieval-crl domain 1
[RouterB] pki request-certificate domain 1
```

配置 IKE 提议 1，使用 rsa-signature 方法为身份认证策略。

```
[RouterB] ike proposal 1
[RouterB-ike-proposal-1] authentication-method rsa-signature
[RouterB-ike-proposal-1] quit
```

在 IKE 对等体中引用 PKI 域的配置。

```
[RouterB]ike peer peer
[RouterB-ike-peer-peer]certificate domain 1
```

说明

以上是对 IKE 协商采用 RSA 数字签名认证方法的配置，若希望建立 IPsec 安全通道进行安全通信，还需要进行 IPsec 的相应配置，具体内容请参见“安全配置指导”中“IPsec”。

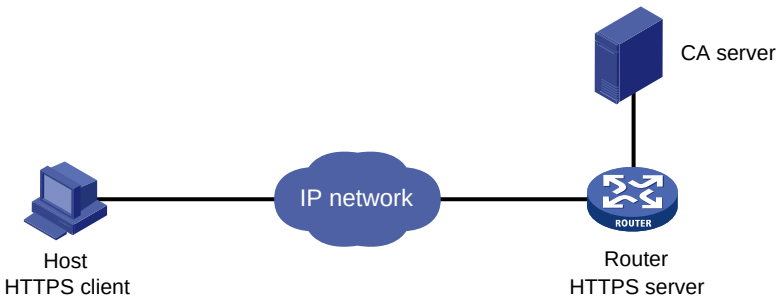
1.12.4 证书属性的访问控制策略应用举例

1. 组网需求

- 客户端通过 HTTPS（HTTP Security，HTTP 安全）协议远程访问设备（HTTPS 服务器）。
- 通过 SSL 协议保证合法客户端安全登录 HTTPS 服务器。
- 为 HTTPS 服务器制定证书属性的访问控制策略，对客户端的访问权限进行控制。

2. 组网图

图1-5 证书属性的访问控制策略应用组网图



3. 配置步骤

说明

- SSL 配置的相关内容请参见“安全配置指导”中的“SSL”。
- HTTPS 配置的相关内容请参见“基础配置指导”中的“配置通过 Web 网管登录设备”。
- SSL策略所引用的PKI域必须首先创建，PKI域参数的具体配置请参见 1.12.1 中的“配置PKI域参数”。

(1) 配置 HTTPS 服务器

配置 HTTPS 服务器使用的 SSL 策略。

```
<Router> system-view
[Router] ssl server-policy myssl
[Router-ssl-server-policy-myssl] pki-domain 1
[Router-ssl-server-policy-myssl] client-verify enable
[Router-ssl-server-policy-myssl] quit
```

(2) 配置证书属性组

配置证书属性组 mygroup1，并创建两个属性规则。规则 1 定义证书主题名的 DN 包含字符串 aabbcc；规则 2 定义证书颁发者名中的 IP 地址等于 10.0.0.1。

```
[Router] pki certificate attribute-group mygroup1
[Router-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc
[Router-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1
[Router-pki-cert-attribute-group-mygroup1] quit
```

配置证书属性组 mygroup2，并创建两个属性规则。规则 1 定义证书备用主题名中的 FQDN 不包含字符串 apple；规则 2 定义证书颁发者名的 DN 包含字符串 aabbcc。

```
[Router] pki certificate attribute-group mygroup2
[Router-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn apple
[Router-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc
[Router-pki-cert-attribute-group-mygroup2] quit
```

(3) 配置证书访问控制策略

配置访问控制策略 myacp，并建立两个控制规则。

```
[Router] pki certificate access-control-policy myacp
[Router-pki-cert-acp-myacp] rule 1 deny mygroup1
[Router-pki-cert-acp-myacp] rule 2 permit mygroup2
[Router-pki-cert-acp-myacp] quit
```

(4) 配置 HTTPS 服务器与相关策略进行关联，并启动 HTTPS 服务器

配置指定 HTTPS 服务器的 SSL 策略为 myssl。

```
[Router] ip https ssl-server-policy myssl
```

配置指定 HTTPS 服务器的证书访问控制策略为 myacp。

```
[Router] ip https certificate access-control-policy myacp
```

启动 HTTPS 服务器。

```
[Router] ip https enable
```

1.13 常见配置错误举例

1.13.1 获取CA证书失败

1. 故障现象

获取 CA 证书时失败。

2. 故障分析

可能有以下原因：

- 网络连接故障，如网线折断，接口松动；
- 没有设置信任的 CA 名称；
- 证书申请的注册服务器 URL 位置不正确或未配置；
- 没有配置证书申请注册受理机构；
- 设备的系统时钟与 CA 的时钟不同步。

3. 处理过程

- 排除物理连接故障；
- 查看各必配项是否都正确配置；
- 可通过 **ping** 命令测试注册服务器是否连接正常；
- 配置证书申请注册受理机构；
- 保持系统时钟与 CA 同步。

1.13.2 本地证书申请失败

1. 故障现象

手工证书请求失败。

2. 故障分析

可能有以下原因：

- 网络连接故障，如网线折断，接口松动；
- 申请之前没有先获取 CA 证书；
- 当前的密钥对已经绑定证书；
- 没有设置信任的 CA 名称；
- 证书申请的注册服务器 URL 位置不正确或未配置；
- 没有配置证书申请注册受理机构；
- 没有配置实体 DN 中必配参数。

3. 处理过程

- 排除物理连接故障；
- 获取 CA 证书；
- 重新创建密钥对；
- 配置信任的 CA 名称；
- 可通过 **ping** 命令测试注册服务器是否连接正常；
- 配置证书申请注册受理机构；

- 可通过查看 CA/RA 注册策略选择相关的实体 DN 属性进行配置。

1.13.3 CRL获取失败

1. 故障现象

获取 CRL 发生失败。

2. 故障分析

可能有以下原因：

- 网络连接故障，如网线折断，接口松动；
- 获取 CRL 之前未先取得 CA 证书；
- 未设置 LDAP 服务器的 IP 地址；
- 未设置 CRL 发布点位置；
- LDAP 服务器版本配置错误。

3. 处理过程

- 排除物理连接故障；
- 获取 CA 证书；
- 设置 LDAP 服务器的 IP 地址；
- 设置 CRL 发布点位置；
- 重新配置 LDAP 版本。