DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers

First Published: November 13, 2009

Last Updated: November 29, 2010

Cisco IOS Release 12.2(33)SCC provides support for certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) in Data-over-Cable Service Interface Specifications (DOCSIS) 3.0 environment on the Cisco CMTS routers enabling you to validate the certificates issued by the certificate authority (CA) for secure transactions.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for DOCSIS 3.0 CRL and OCSP

- The cable modems must be DOCSIS 1.1 and above.
- Baseline Privacy Interface Plus (BPI+) must be enabled.
- The system clock on the Cisco uBR10012 universal broadband router should be set to a current date and time to ensure that system logs have the proper timestamp and to ensure that the BPI+ subsystem uses the correct timestamp for verifying cable modem digital certificates.

This table shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 1: DOCSIS 3.0 CRL and OCSP Feature Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [1]

1 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

Restrictions for DOCSIS 3.0 CRL and OCSP

The DOCSIS 3.0 CRL and OCSP have the following restrictions and limitations:

- The OCSP responder does not verify the validity of the certificate. It only verifies the revocation status of the certificate.
- When the OCSP status of a certificate is unknown to the CMTS, the certificate is treated as “valid”.
- When the CMTS fails to receive the OCSP or CRL response, the certificate is considered as “valid”.
- You cannot specify more than a single server for each protocol.

Information About DOCSIS 3.0 CRL and OCSP

The following sections describe the DOCSIS 3.0 CRL and OCSP support:

Feature Overview

CRL and OCSP are two methods used to check the revocation status of certificates that the certification authority (CA) issues.

CRL is a single signed file that lists the revocation status of certificates. The status includes the date of certificate revocation, time of CRL file creation, and time of release of the next CRL file.

OCSP is the alternative to the CRL. OCSP checks the certificate status at the external OCSP responder for each individual CA and CM certificate. The OCSP responder signs each response and the CMTS validates it.

Certificate Revocation List

Certificate revocation lists are used to check the revocation status of certificates when using a public key infrastructure (PKI) for maintaining access to servers in a network. When there is an attempt to access the server, the access action (allow or deny) is taken based on the specified CRL entry.

The CMTS retrieves the CRL files using HTTP. The retrieved files are checked with a trusted CA to ascertain the validity of the CRL file. If the CMTS cannot verify the validity of the CRL file, it discards the CRL file.

The CMTS employs the following validation process to check the validity of a CA certificate or CM certificate:

- The CMTS uses the current CRL file and attempts to retrieve the subsequent CRL file as indicated in the next-update value in the current CRL file. If the attempt fails, the CMTS continues to use the existing file and attempts to retrieve the new file at periodic intervals.
- If the next-update value is missing from the current CRL file, the CMTS uses the value configured for the CRL file.

Note The next-update value is contained in the CRL file itself.

For more details on CRL feature, refer to the What Is a CRL? section in Configuring Authorization and Revocation of Certificates in a PKI guide.

Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is an alternative to Certificate Revocation Lists. It provides timely information regarding the revocation status of a digital certificate. Unlike CRL, OCSP downloads the revocation status for each CA and CM certificate individually. Because of this, any changes to the revocation states are noted quickly, but at the expense of the additional overhead of contacting the server for each certificate.

When the CMTS receives a CA certificate or CM certificate, it sends a status request to an OCSP responder using the OCSP protocol to check the revocation state of the certificate. The OCSP responder sends the

response as “good”, “revoked”, or “unknown” after checking the revocation status of the certificate in its database. The CMTS uses the response from OCSP responder for the certificate validation process.

The CMTS uses the following validation process to check the validity of a CA certificate or cable modem (CM) certificate:

- The CMTS checks the OCSP response for the next-update value. If the next-update value is available, the CMTS acts as an OCSP client and caches the response status of the certificate. Next, the CMTS attempts to retrieve the revocation status of the certificate only after the time indicated in the next-update value.
- If next-update value is not available in the OCSP response, the CMTS does not cache the OCSP revocation status of the certificate and checks for the certificate validity every time a certificate validation is requested. This is a very resource-intensive method as the certificate validity is checked on a regular basis.

The CMTS sends an OCSP request when a CA certificate or CM certificate is obtained. The request is sent only when the CMTS is configured with OCSP responder information and does not posses a valid certificate status in its cache.

The CMTS treats the certificate as “valid” when:

- The CMTS is unable to retrieve the certificate status.
- The status of the certificate is “unknown”.
- The CMTS fails to receive any response from the OCSP responder.

For more details on OCSP feature, refer to the Online Certificate Status Protocol (OCSP) guide.

How to Configure DOCSIS 3.0 CRL and OCSP

This section describes the following tasks that are required to implement DOCSIS 3.0 CRL and OCSP support:

Configuring Trustpoints

This section describes how to configure trustpoints for CRL and OCSP.

Configuring a Trustpoint

This section describes how to configure trustpoints. Use the cable privacy revocation enable command at the global configuration mode to create the trustpoints and add the certificates for revocation checking.

The cable privacy revocation enable command creates the necessary trustpoints for proper DOCSIS operation. Specify the correct CRL Distribution Point and OCSP responder to configure these trustpoints.

Note IOS is based on trustpoints and the certificates configured in the system refer to this trustpoint.

For information on creating trustpoints, see the Configuring Certificates chapter of the Cisco Security Appliance Command Line Configuration Guide .

Note To set the timeout value of CRL or OCSP response time for authorization messages, use the cable privacy revocation timeout command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation enable** **Example:** `Router(config)# cable privacy revocation enable`	Creates the trustpoints and adds the certificates for revocation checking.
Step 4	**cable privacy revocation timeout** **Example:** `Router(config)# cable privacy revocation timeout`	(Optional) Allows the CMTS to set the timeout value of OCSP response time.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to the privileged EXEC mode.

Configuring DOCSIS Trustpoints

The trustpoints for the US (DOCSIS-US-TRUSTPOINT) and EU (DOCSIS-EU-TRUSTPOINT) root certificates are created dynamically and are used to verify all the manufacturer and CM certificates.

For information on creating trustpoints, see the Configuring Trustpoints section of Configuring Certificates chapter of the Cisco Security Appliance Command Line Configuration Guide.

Tip Use the CRL URL and the OCSP URL to add additional trustpoints. CableLabs and ComLabs also provide a public URL that contains DOCSIS root certificates signed for OCSP responses.

Configuring OCSP

Note The server specified using the ocsp url command is used only when the URL is not specified in the certificate.

To allow the CMTS to skip the OCSP response signature check, use the **cable privacy revocation ocsp skip-sig-check** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable privacy revocation ocsp skip-sig-check**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation ocsp skip-sig-check** **Example:** `Router(config)# cable privacy revocation ocsp skip-sig-check`	Allows the CMTS to skip the OCSP response signature check.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring CRL

This section describes how to configure CRL. For information on Configuring CRL, see the Configuring CRLs for a Trustpoint section of Configuring Certificates document.

Note The server specified using the crl query command is used only when the URL is not specified in the certificate.

To allow the CMTS to skip the CRL response signature check, use the cable privacy revocation crl skip-sig-check command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation crl skip-sig-check** **Example:** `Router(config)# cable privacy revocation ocsp skip-sig-check`	Allows the CMTS to skip the CRL response signature check.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Disabling OCSP Nonce

For information on disabling OCSP Nonce, see the Disabling OCSP Nonces section of Configuring PKI Using the IPSec VPN SPA document.

Note This feature is enabled by default in IOS.

Obtaining Certificates

For information on obtaining certificates, see the Obtaining Certificates section of Configuring Certificates document.

Note The trustpoint needs a public or private keypair to sign the OCSP requests. This key should be made known to the OCSP responder to verify the request. However, signing the request is optional and the OCSP responders do not normally check the validity of the requests.

The OCSP method of checking the certificate status for each individual CA and CM certificate in real-time consumes more resources with resultant performance problems. To mitigate performance related problems, you can disable checking of the CM certificates using the **cable privacy revocation skip-cm-cert** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation skip-cm-cert** **Example:** `Router(config)# cable privacy revocation skip-cm-cert`	Allows the CMTS to disable checking of CM certificates.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Monitoring the DOCSIS 3.0 CRL and OCSP

To verify certificate and trustpoint information, perform the following steps:

Verifying Certificates

To display the certificates that are currently used on the CMTS, use the **show crypto pki certificates** command.

Verifying Certificate Revocation Lists

To display the certificate revocation lists that are currently used on the CMTS, use the **show crypto pki crls** command.

For information on verifying certificate revocation lists, see the Configuring Certificate Authorization and Revocation Settings section of the Configuring Authorization and Revocation of Certificates in a PKI document.

Configuration Examples for DOCSIS 3.0 CRL and OCSP

This section lists the following sample configurations for the DOCSIS 3.0 CRL and OCSP feature on a Cisco CMTS router:

Creating Trustpoints Examples

The following sample configuration shows typical example of a router configured to use trustpoints and optionally sets the timeout value for authorization messages:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation enable
Router(config)# cable privacy revocation timeout
Router(config)# end
```

OCSP Configuration Examples

The following sample configuration shows typical example of a router configured to skip the OCSP response signature check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation ocsp skip-sig-check
Router(config)# end
```

CRL Configuration Examples

The following sample configuration shows typical example of a router configured to skip the CRL response signature check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation crl skip-sig-check
Router(config)# end
```

Obtaining Certificates Configuration Examples

The following sample configuration shows typical example of a router configured to skip the CM certificate check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation skip-cm-cert
Router(config)# end
```

Additional References

The following sections provide references related to the DOCSIS 3.0 CRL and OCSP feature.

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Configuring Certificates	Cisco Security Appliance Command Line Configuration Guide
Security commands	Cisco IOS Security Command Reference
What is OCSP?	Configuring Authorization and Revocation of Certificates in a PKI
CMTS MIBs	Cisco CMTS Universal Broadband Router Series MIB Specifications Guide 12.2SC

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• IF-MIB • DOCS-IF3-MIB • DOCS-SEC-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs For information on MIBs, see http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html Cisco CMTS Universal Broadband Router Series MIB Specifications Guide 12.2SC.

RFCs

RFCs[2]	Title
RFC 3280	Internet X.509 Public Key Infrastructure CRL
RFC 2616	HTTP/1.1
RFC 2560	X.509 Internet Public Key Infrastructure OCSP

2 Not all supported RFCs are listed.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for DOCSIS 3.0 CRL and OCSP for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers	12.2(33)SCC	This feature was introduced for the Cisco uBR10012 universal broadband router. The following commands are new or modified: • **cable privacy revocation crl skip-sig-check** • **cable privacy revocation enable** • **cable privacy revocation ocsp skip-sig-check** • **cable privacy revocation skip-cm-cert** • **cable privacy revocation timeout**