CPE Wan Management Protocol (CWMP)

bintec-Dm 826-I

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents

bintec-Dm 704-I Configuration and Monitoring

Chapter 1 Introduction

1.1 Introduction

1.1.1 CPE Wan Management Protocol

The CPE WAN Management Protocol is intended to be used in communications between a CPE (Customer Premises Equipment) and an Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

A variety of functionalities are supported to manage a collection of CPEs, including primary capabilities like auto-configuration and dynamic service provisioning, software/firmware image management, software module management, status and performance monitoring or diagnostics.

The provisioning mechanism allows for CPE provisioning when initial connection to the broadband access network is established, and the ability to re-provision or re-configure at any subsequent time. This includes support for asynchronous ACS-initiated re-provisioning of a CPE.

The identification mechanisms included in the protocol allow for CPE provisioning based on the requirements of each specific CPE or on collective criteria (such as the CPE vendor, model, software version, etc.).

The protocol also provides optional tools to manage the CPE-specific components of optional applications or services that an additional level of security is required to control (such as those involving payments).

CWMP provides tools to manage the downloading of CPE software/firmware image files. The protocol provides mechanisms for version identification, file download initiation (both for ACS and CPE initiated downloads), and ACS notifications on the success or failure of a file download. It also enables an ACS to manage modular software and execution environments on a CPE. Some of the features it provides include the ability to install, update, and uninstall software modules, as well as to send notifications to the ACS on the success or failure of each action. The protocol also provides support when running or stopping applications on the CPE, enables and disables execution environments, and inventories the software modules available on the device.

Moreover, the ACS can use CPE-supported status and performance statistics to monitor the device. The protocol also defines a set of mechanisms that allow the CPE to notify the ACS of changes to its state.

The protocol also helps a CPE hand information to the ACS that the latter can use to diagnose and resolve connectivity or service issues, as well as carry out predefined diagnostic tests.

1.1.2 Available Functionality in the router

The device has a CWMP client that needs to be managed by means of a configured ACS. It is also equipped with a simple server whose aim is to accept incoming connection requests from the configuration server.

The supported transport modes are TCP and TLS (where required).

Chapter 2 Configuration

2.1 Accessing the Configuration Menu

The CPE Wan Management Protocol configuration commands must be entered in the configuration menu associated with the CWMP (*CWMP Config>*). To access said menu, use the **feature cwmp** command found in the general configuration menu (*Config>*).

```
Config>feature cwmp

-- CPE WAN Management Protocol configuration --
CWMP Config>
```

If you want the commands to activate immediately (i.e. without rebooting the router), access the configuration through the dynamic general configuration menu (*Config$*).

```
Config$feature cwmp

-- CPE WAN Management Protocol configuration --
CWMP Config$
```

2.2 CWMP Menu Configuration Commands

2.2.1 [NO] LOCAL

Configuration commands related to the internal server.

Syntax:

```
CWMP Config$[no] local <option>
```

```
CWMP Config$[no] local ?
  ip-address    Specifies the IP used to listen ACS connection request
  password      Specifies the password used by ACS at connection request
  user          Specifies the user used by ACS at connection request
  vrf           VRF instance name
CWMP Config$
```

2.2.1.1 LOCAL IP-ADDRESS

Configures the IP address that the internal server uses to listen for incoming connection requests from the ACS. If this command is not configured, the internal server will not be enabled.

Syntax:

```
CWMP Config$[no] local ip-address <option>
```

```
CWMP Config$[no] local ip-address ?
  <a.b.c.d>      Ipv4 format
  <interface>    Interface name
CWMP Config$
```

2.2.1.1.1 <a.b.c.d>

This option is used to configure an IP address directly for the service.

Syntax:

```
CWMP Config$[no] local ip-address <a.b.c.d>    Ipv4 format
```

Example:

```
CWMP Config$local ip-address 192.168.1.1
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.1.1.2 <interface>

This option is used to configure an interface address for the service. The IP address of said interface is used for the service.

Syntax:

```
CWMP Config$[no] local ip-address <interface>    Interface name
```

Example:

```
CWMP Config$local ip-address ethernet0/0
```

Command history:

Release	Modification
11.01.03	New option added.

2.2.1.2 LOCAL PASSWORD

Configures the password used by the internal server to authenticate incoming connections. If this command is not configured, the internal server (when enabled) will accept all incoming connections. It can be configured as plain or ciphered text.

Syntax:

```
CWMP Config$[no] local password <plain | cipher> <string>
```

Example:

```
CWMP Config$local password plain pass
```

```
CWMP Config$local password ciphered 0x163FE1EE75E6A3BD
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.1.3 LOCAL USER

Configures the user the internal server employs to authenticate incoming connections. If this command is not configured, the internal server (when enabled) will accept all incoming connections.

Syntax:

```
CWMP Config$[no] local user <string>
```

Example:

```
CWMP Config$local user localcpe
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.1.4 LOCAL VRF

Configures the VRF (VPN routing/forwarding) instance used to listen to, and receive, incoming connections from the ACS. This option is not configured by default and the main VRF instance is used.

Syntax:

```
CWMP Config$[no] local vrf <1..32 chars>
```

Example:

```
CWMP Config$local vrf cwmp_vrf
```

Command history:

Release	Modification
11.01.03	New command added.

2.2.2 [NO] MANAGEMENT-SERVER

Configuration commands related to CPE client management.

Syntax:

```
CWMP Config$[no] management-server <option>
```

```
CWMP Config$management-server ?
  ca                     CA certificate for server validation
  dev-cert               Device certificate to be validated at server
  password               Specifies the ACS password that is used in the authentication phase
  periodic-interval      Specifies the interval used to transmit Inform messages periodically
  url                    Specifies the HTTP/HTTPS URL to reach the ACS
  user                   Specifies the ACS user that is used in the authentication phase
  version-release        Specifies the release version used by the CWMP (v. 1.x)
  vrf                    VRF instance name
CWMP Config$
```

2.2.2.1 MANAGEMENT-SERVER CA

Configures the certification authority that is valid for TLS sessions established through the CWMP protocol. This needs to be configured if the ACS connection is secured (HTTPS).

The certification authority allows you to validate device certificates and sends this information to the router through TLS.

Syntax:

```
CWMP Config$[no] management-server ca <option>
```

```
CWMP Config$management-server ca ?
  cert-name      Certificate name
  dont-verify    Disable validation of CA certificate
  scep-cert      Certificate obtained via SCEP
CWMP Config$
```

2.2.2.1.1 CERT-NAME

This option is used to configure the file name of the CA certificate.

Syntax:

```
CWMP Config$[no] management-server ca cert-name <ca-name>
```

To load a certificate in base64, you can enter the **certificate <certname> base64** command and insert the certificate through the device's ipsec certificate menu. This generates an ipsec configuration, as shown in the example. Another option is to use SCEP to obtain the certificate from a configured server. For further details, please see the section on Certificates (chapter 2) in manual bintec-Dm739-I IPSEC.

Example:

Loading a bintec example root certificate through the **certificate <name> base64** command in the *protocol ip>ipsec>cert* menu.

```
CERTIFICATES config$certificate CA.CER base64

Introduce the Certificate (Base 64 format)
Enter <cr> to escape
-----BEGIN CERTIFICATE-----
MIIEmzCCA4OgAwIBAgIJAIjCeKBqciDFMA0GCSqGSIb3DQEBBAUAMIGPMQswCQYD
VQQGEwJTUDEPMA0GA1UECBMGTWFkcmlkMRQwEgYDVQQHEwtUcmVzIENhbnRvczEU
```

```
MBIGA1UEChMLVGVsZGF0IFMuQS4xGzAZBgNVBAsTEklQIFRlbGVwaG9ueSBHcm91
cDEmMCQGA1UEAxMdVGVkYXQgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMDcw
NjExMTUxNDE2WhcNMTcwNjA4MTUxNDE2WjCBjzELMAkGA1UEBhMCU1AxDzANBgNV
BAgTBk1hZHJpZDEUMBIGA1UEBxMLVHJlcyBDYW50b3MxFDASBgNVBAoTC1RlbGRh
dCBTLkEuMRswGQYDVQQLExJJUCBUZWxlcGhvbnkgR3JvdXAxJjAkBgNVBAMTHVRl
ZGF0IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAmSRtZ9wHCksPAzkdMvqYyUAnOecJWw/Aai67TObXhi/a4w5T
Onbf8LKjsGWamksMU6p7iv7n4rd6Kqyr1q/S1yP9XfENiVfsmu3dq9ehkipg5ixw
E16xAdpGXJpdob8zOkUwiKaJib8LsTE38upaA2iV++bQSIMKcma4rnlPW1wn9jAJ
mMwTMKCT7vT7OfcEIVzB7P1RW9phTMmQsSTTg7SMlRxTN0c2WW216aLOO5qRwvt4
xzcoXRVYbm2aBj7LucjsOrgoEdscmga8kK7PYdetxqti1n6RfjP2BXmAUrKh91c3
61fazv+pNxpKSL0hQ8Gb+hUxPyjZJTTW+Zih+wIDAQABo4H3MIH0MB0GA1UdDgQW
BBQsJNVrUzOnr7Rxj4FfdiBLKOSv9DCBxAYDVR0jBIG8MIG5gBQsJNVrUzOnr7Rx
j4FfdiBLKOSv9KGBlaSBkjCBjzELMAkGA1UEBhMCU1AxDzANBgNVBAgTBk1hZHJp
ZDEUMBIGA1UEBxMLVHJlcyBDYW50b3MxFDASBgNVBAoTC1RlbGRhdCBTLkEuMRsw
GQYDVQQLExJJUCBUZWxlcGhvbnkgR3JvdXAxJjAkBgNVBAMTHVRlZGF0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5ggkAiMJ4oGpyIMUwDAYDVR0TBAUwAwEB/zANBgkq
hkiG9w0BAQQFAAOCAQEAR16Gjs16Sqz04v/RJeRb+fcbKvAgzO3sWpUyYwzU/j6L
7R5XVbgimX4FQ3qxnrNeYXCTtZAM8yMWKpnX1d9ZDgGqZsOV0NrjlSGAYk3yvdM5
cNEXQpLDkKhjN8ageD48yNWpBTzbTDk/jQXCfktF3L93qpB/W76taC54bb1LojHs
kcPXB4pzgN7QGct/wVyg2KNcMaQITmOesY+Qqt8T0QxZomsn8ldz6c7HAoRurmnB
x/SCdpqfwMMnS7ap/5y+uPNuROw3ib8GWWqq6I3/bUqxgkgEwWD8OdkYHKNJV5h8
0zJjXH5/jqf1hmwKV07QQ+WxENxdtc6FB3Idmgj33w==
-----END CERTIFICATE-----
```

The certificate data can be seen through the **list loaded-certificates** command found in this menu. If you have loaded the certificate using static configuration, you’ll need to save it and restart the device in order to save it in the memory.

```
CERTIFICATES config$list loaded-certificates
----------------------- CA.CER (from config)
 Subject:
  CN (Common Name        ): bintec Certification Authority
  OU (Organizational Unit): IP Telephony Group
  O  (Organization Name  ): bintec
  L  (Locality           ): Tres Cantos
  S  (State or Province  ): Madrid
  C  (Country Name       ): SP

 Issuer: A: CA.CER

CERTIFICATES config$
```

This has generated the following configuration in the certificates menu. This configuration can be entered into another device without having to reload the certificate in base64.

```
protocol ip
; -- Internet protocol user configuration –
   Ipsec
; -- IPSec user configuration --
      Cert
; -- Cert user configuration --
         file new CA.CER
         file add 0x3082049B30820383A0030201020209008C278A06A7220C5300D06092A864886
         file add 0xF70D010104050030818F310B3009060355040613025350310F300D0603550408
         file add 0x13064D616472696431143012060355040713OB547265732043616E746F733114
         file add 0x3012060355040A130B54656C64617420532E412E311B3019060355040B131249
         file add 0x502054656C6570686F6E792047726F75703126302406035504031310D54656461
         file add 0x74204365727469666963617469F6E20417574686F72697479301E170D303730
         file add 0x3631313135313431365A170D3137303630383135313431365A30818F310B3009
         file add 0x0603550406130253503 10F300D06035504081306 4D616472696431143012060 3
         file add 0x550407130B547265732043616E746F733114301206035504 0A130B54656C6461
         file add 0x7420532E412E311B3019060355040B131249502054656C6570686F6E79204772
         file add 0x6F7570312630240603550403131D546564617420436572746966696361 74696F
         file add 0x6E20417574686F72697479308201 22300D06092A864886F70D01010105000382
         file add 0x010F003082010A028201010099246D67DC070A4B0F03391D32FA98C9402739E7
         file add 0x095B0FC06A2EBB4CE6D7862FDAE30E533A76DFF0B2A3B0659A9A4B0C53AA7B8A
         file add 0xFEE7E2B77A2AACABD6AFD2D723FD5DF10D8957EC9AEDDDABD7A1922A60E62C70
         file add 0x135EB101DA465C9A5DA1BF333A453088A68989BF0BB13137F2EA5A036895FBE6
         file add 0xD048830A7266B8AE794F5B5C27F6300998CC1330A093EEF4FB39F704215CC1EC
         file add 0xFD515BDA614CC990B124D383B48C951C53374736596DB5E9A2CE3B9A91C2FB78
         file add 0xC737285D15586E6D9A063ECBB9C8EC3AB82811DB1C9A06BC90AECF61D7ADC6AB
         file add 0x62D67E917E33F605798052B2A1F75737EB57DACEFFA9371A4A48BD2143C19BFA
         file add 0x15313F28D92534D6F998A1FB0203010001A381F73081F4301D0603551D0E0416
         file add 0x04142C24D56B5333A7AFB4718F815F76204B28E4AFF43081C40603551D230481
         file add 0xBC3081B980142C24D56B5333A7AFB4718F815F76204B28E4AFF4A18195A48192
         file add 0x30818F310B3009060355040613025350310F300D060355040813064D61647269
         file add 0x643114301206035504071300B547265732043616E746F7331143012060355040A
         file add 0x130B54656C64617420532E412E311B3019060355040B131249502054656C6570
         file add 0x686F6E792047726F7570312630240603550403131D54656461742043657274
         file add 0x6669636174696F6E20417574686F726974798209008C278A06A7220C5300C06
         file add 0x03551D13040530030101FF300D06092A864886F70D0101040500038201010047
         file add 0x5E868ECD7A4AACF4E2FFD125E45BF9F71B2AF020CCEDEC5A9532630CD4FE3E8B
         file add 0xED1E5755B822997E05437AB19EB35E617093B5900CF323162A99D7D5DF590E01
         file add 0xAA66C395D0DAE3952180624DF2BDD33970D1174292C390A86337C6A0783E3CC8
         file add 0xD5A9053CDB4C393F8D05C27E4B45DCBF77AA907F5BBEAD682E786DBD4BA231EC
         file add 0x91C3D7078A7380DED019CB7FC15CA0D8A35C31A4084E639EB18F90AADF13D10C
         file add 0x59A26B27F25773E9CEC702846EAE69C1C7F482769A9FC0C3274BB6A9FF9CBEB8
         file add 0xF36E44EC3789BF06596AAAE88DFF6D4AB1824804C160FC39D9181CA34957987C
         file end 0xD332635C7E7F8EA7F5866C0A574ED043E5B110DC5DB5CE8507721D9A08F7DF
;
         certificate CA.CER load
      exit
;
   exit
;
exit
```

Now, all you need to do is to configure this certificate as a trusted certification authority for CWMP protocol TLS connections.

```
CWMP Config$management-server ca cert-name CA.CER
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.1.2 DONT-VERIFY

If this option is active, the client does not verify if the server's X509 certificate is signed by a trustworthy certification authority. This option is not enabled by default and the device checks that the server certificate has been signed by a reliable authority.

Syntax:

```
CWMP Config$[no] management-server ca dont-verify
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.1.3 SCEP-CERT

This option is mandatory if certificates are obtained via SCEP. If it is active, the CWMP client will wait without fully establishing the session until the SCEP process obtains the server's CA X509 certificate and it can be used. This option is not enabled by default and the client will drop the session if, during its check, the CA certificate configured is not available.

Syntax:

```
CWMP Config$[no] management-server ca scep-cert
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.2 MANAGEMENT-SERVER DEV-CERT

Configures the client's certificate that must be validated during TLS sessions established through the CWMP protocol. This option needs to be configured if the ACS connection is secured (HTTPS) and the ACS requires the use of the client's certificate.

Thanks to this certificate, the device can be validated by an ACS server through TLS.

Syntax:

```
CWMP Config$[no] management-server dev-cert <option>
```

```
CWMP Config$management-server dev-cert ?
  ca-cert-name CA certificate name that signs the device certificate
  scep-cert    Certificate obtained via SCEP
CWMP Config$
```

2.2.2.2.1 CERT-NAME

This option is used to configure the file name of the device's certificate.

Syntax:

```
CWMP Config$[no] management-server dev-cert cert-name <certname>
```

To load a certificate in base64, you can enter the **certificate <certname> base64** command and insert the certificate through the device's ipsec certificate menu. This generates an ipsec configuration, as shown in the example. Another option is to use SCEP to obtain the certificate from a configured server. For further details, please see the section on Certificates (chapter 2) in manual bintec-Dm739-I IPSEC.

Example:

Loading a bintec example root certificate through the **certificate <name> base64** command in the *protocol ip>ipsec>cert* menu.

```
CERTIFICATES config$certificate DEVICE.CER base64

Introduce the Certificate (Base 64 format)
Enter <cr> to escape
-----BEGIN CERTIFICATE-----
MIIEmzCCA4OgAwIBAgIJAIjCeKBqciDFMA0GCSqGSIb3DQEBBAUAMIGPMQswCQYD
VQQGEwJTUDEPMA0GA1UECBMGTWFkcmlkMRQwEgYDVQQHEwtUcmVzIENhbnRvczEU
MBIGA1UEChMLVGVsZGF0IFMuQS4xGzAZBgNVBAsTEklQIFRlbGVwaG9ueSBHcm91
cDEmMCQGA1UEAxMdVGVkYXQgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMDcw
NjExMTUxNDE2WhcNMTcwNjA4MTUxNDE2WjCBjzELMAkGA1UEBhMCU1AxDzANBgNV
BAgTBk1hZHJpZDEUMBIGA1UEBxMLVHJlcyBDYW50b3MxFDASBgNVBAoTC1RlbGRh
dCBTLkEuMRswGQYDVQQLExJJUCBUZWxlcGhvbnkgR3JvdXAxJjAkBgNVBAMTHVRl
ZGF0IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAmSRtZ9wHCksPAzkdMvqYyUAnOecJWw/Aai67TObXhi/a4w5T
Onbf8LKjsGWamksMU6p7iv7n4rd6Kqyr1q/S1yP9XfENiVfsmu3dq9ehkipg5ixw
E16xAdpGXJpdob8zOkUwiKaJib8LsTE38upaA2iV++bQSIMKcma4rnlPW1wn9jAJ
mMwTMKCT7vT7OfcEIVzB7P1RW9phTMmQsSTTg7SMlRxTN0c2WW216aLOO5qRwvt4
xzcoXRVYbm2aBj7LucjsOrgoEdscmga8kK7PYdetxqti1n6RfjP2BXmAUrKh91c3
61fazv+pNxpKSL0hQ8Gb+hUxPyjZJTTW+Zih+wIDAQABo4H3MIH0MB0GA1UdDgQW
BBQsJNVrUzOnr7Rxj4FfdiBLKOSv9DCBxAYDVR0jBIG8MIG5gBQsJNVrUzOnr7Rx
j4FfdiBLKOSv9KGBlaSBkjCBjzELMAkGA1UEBhMCU1AxDzANBgNVBAgTBk1hZHJp
ZDEUMBIGA1UEBxMLVHJlcyBDYW50b3MxFDASBgNVBAoTC1RlbGRhdCBTLkEuMRsw
GQYDVQQLExJJUCBUZWxlcGhvbnkgR3JvdXAxJjAkBgNVBAMTHVRlZGF0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5ggkAiMJ4oGpyIMUwDAYDVR0TBAUwAwEB/zANBgkq
hkiG9w0BAQQFAAOCAQEAR16Gjs16Sqz04v/RJeRb+fcbKvAgzO3sWpUyYwzU/j6L
7R5XVbgimX4FQ3qxnrNeYXCTtZAM8yMWKpnX1d9ZDgGqZsOV0NrjlSGAYk3yvdM5
cNEXQpLDkKhjN8ageD48yNWpBTzbTDk/jQXCfktF3L93qpB/W76taC54bb1LojHs
kcPXB4pzgN7QGct/wVyg2KNcMaQITmOesY+Qqt8T0QxZomsn8ldz6c7HAoRurmnB
x/SCdpqfwMMnS7ap/5y+uPNuROw3ib8GWWqq6I3/bUqxgkgEwWD8OdkYHKNJV5h8
0zJjXH5/jqf1hmwKV07QQ+WxENxdtc6FB3Idmgj33w==
-----END CERTIFICATE-----
```

The certificate data can be seen through the **list loaded-certificates** command found in this menu. If you have loaded the certificate using static configuration, you'll need to save it and restart the device in order to save it in the memory.

```
CERTIFICATES config$list loaded-certificates
----------------------- DEVICE.CER (from config)
 Subject:
  CN (Common Name        ): bintec Certification Authority
  OU (Organizational Unit): IP Telephony Group
  O  (Organization Name  ): bintec
  L  (Locality           ): Tres Cantos
  S  (State or Province  ): Madrid
  C  (Country Name       ): SP

 Issuer: A:DEVICE.CER

CERTIFICATES config$
```

This has generated the following configuration in the certificates menu. This configuration can be entered into another device without having to reload the certificate in base64.

```
protocol ip
; -- Internet protocol user configuration –
   Ipsec
; -- IPSec user configuration --
      Cert
; -- Cert user configuration --
         file new DEVICE.CER
         file add 0x3082049B30820383A00302010202090088C278A06A7220C5300D06092A864886
         file add 0xF70D010104050030818F310B3009060355040613025350310F300D0603550408
         file add 0x13064D6164726964311430120603550407130B547265732043616E746F733114
         file add 0x3012060355040A130B54656C64617420532E412E311B3019060355040B131249
         file add 0x502054656C6570686F6E792047726F7570312630240603550403131D54656461
         file add 0x742043657274696669636174696F6E20417574686F72697479301E170D303730
         file add 0x3631313135313431365A170D3137303630383135313431365A30818F310B3009
         file add 0x060355040613025350310F300D060355040813064D6164726964311430120603
         file add 0x550407130B547265732043616E746F7331143012060355040A130B54656C6461
         file add 0x7420532E412E311B3019060355040B131249502054656C6570686F6E79204772
         file add 0x6F7570312630240603550403131D54656461742043657274696669636174696F
         file add 0x6E20417574686F7269747930820122300D06092A864886F70D01010105000382
         file add 0x010F003082010A028201010099246D67DC070A4B0F03391D32FA98C9402739E7
         file add 0x095B0FC06A2EBB4CE6D7862FDAE30E533A76DFF0B2A3B0659A9A4B0C53AA7B8A
         file add 0xFEE7E2B77A2AACABD6AFD2D723FD5DF10D8957EC9AEDDDABD7A1922A60E62C70
         file add 0x135EB101DA465C9A5DA1BF333A453088A68989BF0BB13137F2EA5A036895FBE6
         file add 0xD048830A7266B8AE794F5B5C27F6300998CC1330A093EEF4FB39F704215CC1EC
         file add 0xFD515BDA614CC990B124D383B48C951C53374736596DB5E9A2CE3B9A91C2FB78
         file add 0xC737285D15586E6D9A063ECBB9C8EC3AB82811DB1C9A06BC90AECF61D7ADC6AB
         file add 0x62D67E917E33F605798052B2A1F75737EB57DACEFFA9371A4A48BD2143C19BFA
         file add 0x15313F28D92534D6F998A1FB0203010001A381F73081F4301D0603551D0E0416
         file add 0x04142C24D56B5333A7AFB4718F815F76204B28E4AFF43081C40603551D230481
         file add 0xBC3081B980142C24D56B5333A7AFB4718F815F76204B28E4AFF4A18195A48192
         file add 0x30818F310B3009060355040613025350310F300D060355040813064D61647269
         file add 0x64311430120603550407130B547265732043616E746F7331143012060355040A
         file add 0x130B54656C64617420532E412E311B3019060355040B131249502054656C6570
         file add 0x686F6E792047726F7570312630240603550403131D5465646174204365727469
         file add 0x6669636174696F6E20417574686F7269747982090088C278A06A7220C5300C06
         file add 0x03551D13040530030101FF300D06092A864886F70D0101040500038201010047
         file add 0x5E868ECD7A4AACF4E2FFD125E45BF9F71B2AF020CCEDEC5A9532630CD4FE3E8B
         file add 0xED1E5755B822997E05437AB19EB35E617093B5900CF323162A99D7D5DF590E01
         file add 0xAA66C395D0DAE3952180624DF2BDD33970D1174292C390A86337C6A0783E3CC8
         file add 0xD5A9053CDB4C393F8D05C27E4B45DCBF77AA907F5BBEAD682E786DBD4BA231EC
         file add 0x91C3D7078A7380DED019CB7FC15CA0D8A35C31A4084E639EB18F90AADF13D10C
         file add 0x59A26B27F25773E9CEC702846EAE69C1C7F482769A9FC0C3274BB6A9FF9CBEB8
         file add 0xF36E44EC3789BF06596AAAE88DFF6D4AB1824804C160FC39D9181CA34957987C
         file end 0xD332635C7E7F8EA7F5866C0A574ED043E5B110DC5DB5CE8507721D9A08F7DF
;
         certificate DEVICE.CER load
      exit
;
   exit
;
exit
```

Now, all you need to do is to configure this certificate as the device's certificate for CWMP protocol TLS connections.

```
CWMP Config$management-server dev-cert cert-name DEVICE.CER
```

Command history:

Release	Modification
11.01.02	New command added.
11.01.05	This command option has been obsoleted and replaced by the new "ca-cert-name" option described below.

2.2.2.2.2 CA-CERT-NAME

This option is used to configure the file name of the ca certificate that has to sign the device's certificate. The device searches for all certificates signed by this ca and uses a valid one as a device certificate.

Syntax:

```
CWMP Config$[no] management-server dev-cert ca-cert-name <certname>
```

To load a certificate in base64, you can enter the **certificate <certname> base64** command and insert the certificate through the device's ipsec certificate menu. This generates an ipsec configuration, as shown in the example. Another option is to use SCEP to obtain the certificate from a configured server. For further details, please see the section on Certificates (chapter 2) in manual bintec-Dm739-I IPSEC.

Example:

Loading a bintec example root certificate through the **certificate <name> base64** command in the *protocol ip>ipsec>cert* menu.

```
CERTIFICATES config$certificate DEVICE-CA.CER base64

Introduce the Certificate (Base 64 format)
Enter <cr> to escape
-----BEGIN CERTIFICATE-----
MIIEmzCCA4OgAwIBAgIJAIjCeKBqciDFMA0GCSqGSIb3DQEBBAUAMIGPMQswCQYD
VQQGEwJTUDEPMA0GA1UECBMGTWFkcmlkMRQwEgYDVQQHEwtUcmVzIENhbnRvczEU
MBIGA1UEChMLVGVsZGF0IFMuQS4xGzAZBgNVBAsTEklQIFRlbGVwaG9ueSBHcm91
cDEmMCQGA1UEAxMdVGVkYXQgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMDcw
NjExMTUxNDE2WhcNMTcwNjA4MTUxNDE2WjCBjzELMAkGA1UEBhMCU1AxDzANBgNV
BAgTBk1hZHJpZDEUMBIGA1UEBxMLVHJlcyBDYW50b3MxFDASBgNVBAoTC1RlbGRh
dCBTLkEuMRswGQYDVQQLExJJUCBUZWxlcGhvbnkgR3JvdXAxJjAkBgNVBAMTHVRl
ZGF0IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAmSRtZ9wHCksPAzkdMvqYyUAnOecJWw/Aai67TObXhi/a4w5T
Onbf8LKjsGWamksMU6p7iv7n4rd6Kqyr1q/S1yP9XfENiVfsmu3dq9ehkipg5ixw
E16xAdpGXJpdob8zOkUwiKaJib8LsTE38upaA2iV++bQSIMKcma4rnlPW1wn9jAJ
mMwTMKCT7vT7OfcEIVzB7P1RW9phTMmQsSTTg7SMlRxTN0c2WW216aLOO5qRwvt4
xzcoXRVYbm2aBj7LucjsOrgoEdscmga8kK7PYdetxqti1n6RfjP2BXmAUrKh91c3
61fazv+pNxpKSL0hQ8Gb+hUxPyjZJTTW+Zih+wIDAQABo4H3MIH0MB0GA1UdDgQW
BBQsJNVrUzOnr7Rxj4FfdiBLKOSv9DCBxAYDVR0jBIG8MIG5gBQsJNVrUzOnr7Rx
j4FfdiBLKOSv9KGBlaSBkjCBjzELMAkGA1UEBhMCU1AxDzANBgNVBAgTBk1hZHJp
ZDEUMBIGA1UEBxMLVHJlcyBDYW50b3MxFDASBgNVBAoTC1RlbGRhdCBTLkEuMRsw
GQYDVQQLExJJUCBUZWxlcGhvbnkgR3JvdXAxJjAkBgNVBAMTHVRlZGF0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5ggkAiMJ4oGpyIMUwDAYDVR0TBAUwAwEB/zANBgkq
hkiG9w0BAQQFAAOCAQEAR16Gjs16Sqz04v/RJeRb+fcbKvAgzO3sWpUyYwzU/j6L
7R5XVbgimX4FQ3qxnrNeYXCTtZAM8yMWKpnX1d9ZDgGqZsOV0NrjlSGAYk3yvdM5
cNEXQpLDkKhjN8ageD48yNWpBTzbTDk/jQXCfktF3L93qpB/W76taC54bb1LojHs
kcPXB4pzgN7QGct/wVyg2KNcMaQITmOesY+Qqt8T0QxZomsn8ldz6c7HAoRurmnB
x/SCdpqfwMMnS7ap/5y+uPNuROw3ib8GWWqq6I3/bUqxgkgEwWD8OdkYHKNJV5h8
0zJjXH5/jqf1hmwKV07QQ+WxENxdtc6FB3Idmgj33w==
-----END CERTIFICATE-----
```

The certificate data can be seen through the **list loaded-certificates** command found in this menu. If you have loaded the certificate using static configuration, you’ll need to save it and restart the device in order to save it in the memory.

```
CERTIFICATES config$list loaded-certificates
----------------------- DEVICE-CA.CER (from config)
 Subject:
  CN (Common Name        ): bintec Certification Authority
  OU (Organizational Unit): IP Telephony Group
  O  (Organization Name  ): bintec
  L  (Locality           ): Tres Cantos
  S  (State or Province  ): Madrid
  C  (Country Name       ): SP

 Issuer: A:DEVICE-CA.CER

CERTIFICATES config$
```

This has generated the following configuration in the certificates menu. This configuration can be entered into another device without having to reload the certificate in base64.

```
protocol ip
; -- Internet protocol user configuration –
   Ipsec
; -- IPSec user configuration --
      Cert
; -- Cert user configuration --
         file new DEVICE-CA.CER
         file add 0x3082049B30820383A00302010202090088C278A06A7220C5300D06092A864886
         file add 0xF70D01010405003081 8F310B3009060355040613025350310F300D0603550408
         file add 0x13064D61647269643114301206035504071 30B547265732043616E746F733114
         file add 0x3012060355040A130B54656C64617420532E412E311B3019060355040B131249
         file add 0x502054656C6570686F6E792047726F757031263024060355040313 1D54656461
         file add 0x74204365727469666963617469 6F6E20417574686F72697479301E170D303730
         file add 0x3631313135313431365A170D31373036303831353134313 65A30818F310B3009
         file add 0x0603550406130253 50310F300D060355040813064D61647269643114301206 03
         file add 0x550407130B547265732043616E746F733114301206035504 0A130B54656C6461
         file add 0x7420532E412E311B3019060355040B13124950205465 6C6570686F6E79204772
         file add 0x6F757031263024060355040313 1D546564617420436572746966696361746 96F
         file add 0x6E20417574686F7269747930820122300D06092A864886F70D01010105000382
         file add 0x010F003082010A0282010100 99246D67DC070A4B0F03391D32FA98C9402739E7
         file add 0x095B0FC06A2EBB4CE6D7862FDAE30E533A76DFF0B2A3B0659A9A4B0C53AA7B8A
         file add 0xFEE7E2B77A2AACABD6AFD2D723FD5DF10D8957EC9AEDDDABD7A1922A60E62C70
         file add 0x135EB101DA465C9A5DA1BF333A453088A68989BF0BB13137F2EA5A036895FBE6
         file add 0xD048830A7266B8AE794F5B5C27F6300998CC1330A093EEF4FB39F704215CC1EC
         file add 0xFD515BDA614CC990B124D383B48C951C53374736596DB5E9A2CE3B9A91C2FB78
         file add 0xC737285D15586E6D9A063ECBB9C8EC3AB82811DB1C9A06BC90AECF61D7ADC6AB
         file add 0x62D67E917E33F605798052B2A1F75737EB57DACEFFA9371A4A48BD2143C19BFA
         file add 0x15313F28D92534D6F998A1FB0203010001A381F73081F4301D0603551D0E0416
         file add 0x04142C24D56B5333A7AFB4718F815F76204B28E4AFF43081C40603551D230481
         file add 0xBC3081B980142C24D56B5333A7AFB4718F815F76204B28E4AFF4A18195A48192
         file add 0x30818F310B3009060355040613025350310F300D060355040813064D61647269
         file add 0x643114301206035504071 30B547265732043616E746F7331143012060355040A
         file add 0x130B54656C64617420532E412E311B3019060355040B131249502054656C6570
         file add 0x686F6E792047726F7570312630240603550403131D546564617420436572746 9
         file add 0x6669636174696F6E20417574686F7269747982090088C278A06A7220C5300C06
         file add 0x03551D13040530030101FF300D06092A864886F70D0101040500038201010047
         file add 0x5E868ECD7A4AACF4E2FFD125E45BF9F71B2AF020CCEDEC5A9532630CD4FE3E8B
         file add 0xED1E5755B822997E05437AB19EB35E617093B5900CF323162A99D7D5DF590E01
         file add 0xAA66C395D0DAE3952180624DF2BDD33970D1174292C390A86337C6A0783E3CC8
         file add 0xD5A9053CDB4C393F8D05C27E4B45DCBF77AA907F5BBEAD682E786DBD4BA231EC
         file add 0x91C3D7078A7380DED019CB7FC15CA0D8A35C31A4084E639EB18F90AADF13D10C
         file add 0x59A26B27F25773E9CEC702846EAE69C1C7F482769A9FC0C3274BB6A9FF9CBEB8
         file add 0xF36E44EC3789BF06596AAAE88DFF6D4AB1824804C160FC39D9181CA34957987C
         file end 0xD332635C7E7F8EA7F5866C0A574ED043E5B110DC5DB5CE8507721D9A08F7DF
;
         certificate DEVICE-CA.CER load
      exit
;
   exit
;
exit
```

Now, all you need to do is to configure this certificate as the ca signer of the device's certificate for CWMP protocol TLS connections.

```
CWMP Config$management-server dev-cert ca-cert-name DEVICE-CA.CER
```

Command history:

Release	Modification
11.01.05	New command added.

2.2.2.2.3 SCEP-CERT

This command is mandatory if certificates are obtained via SCEP. If it is active (and the device's ca certificate option is configured), the CWMP client will wait without fully establishing the session until the SCEP process obtains the device's X509 certificate and it can be used. This option is not enabled by default and the client will drop the session if, during its check, the configured device's certificate is not available.

Syntax:

```
CWMP Config$[no] management-server dev-cert scep-cert
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.3 MANAGEMENT-SERVER PASSWORD

Configures the password used by the CWMP client to authenticate in the ACS. It can be configured as plain or ciphered text.

Syntax:

```
CWMP Config$[no] management-server password <plain | cipher> <string>
```

Example:

```
CWMP Config$management-server password plain pass
```

```
CWMP Config$management-server password ciphered 0x163FE1EE75E6A3BD
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.4 MANAGEMENT-SERVER PERIODIC-INTERVAL

Configures the periodic-interval command so that PERIODIC events are sent to the ACS via recurring messages. The value is the time in seconds the CPE waits in between periodic sessions. By default, this value is set to 0.

Syntax:

```
CWMP Config$[no] management-server periodic-interval <0...3600>
```

Example:

```
CWMP Config$management-server periodic-interval 1200
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.5 MANAGEMENT-SERVER URL

Configures the ACS url to which the CPE client has to connect in order to establish CWMP sessions. If this command is not configured, the CPE client will not be enabled and the CWMP will not work. To secure a connection and trigger encryption mechanisms, configuration must be carried out using url " http://" or "https://". For secured connections, you must also set a valid CA certificate at the *management-server ca* command.

Syntax:

```
CWMP Config$[no] management-server url <string>
```

Example:

```
CWMP Config$management-server url http://acs.example.com/cwmp
```

```
CWMP Config$management-server url https://cwmp.example.com
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.6 MANAGEMENT-SERVER USER

Configures the user the CWMP client employs to authenticate with ACS.

Syntax:

```
CWMP Config$[no] management-server user <string>
```

Example:

```
CWMP Config$management-server user cpeserver
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.2.7 MANAGEMENT-SERVER VERSION-RELEASE

Configures the release version of the CWMP protocol used by CPE to establish a new session. By default, the release version used is 2 (Version 1.2).

Syntax:

```
CWMP Config$[no] management-server version-release <0..2>    version-release
```

Example:

```
CWMP Config$management-server version-release 0
```

Command history:

Release	Modification
11.01.03	New command added.

2.2.2.8 MANAGEMENT-SERVER VRF

Configures the VRF (VPN routing/forwarding) instance used by the CPE client to connect with ACS in order to establish CWMP sessions. This option is not configured by default and the main VRF instance is used.

Syntax:

```
CWMP Config$[no] management-server vrf <1..32 chars>
```

Example:

```
CWMP Config$management-server vrf cwmp_vrf
```

Command history:

Release	Modification
11.01.03	New command added.

2.2.3 [NO] PROVISION-CODE

Configures the value used by the CPE for the DeviceInfo.ProvisioningCode parameter of the tr069 InternetGatewayDevice data model. By default, this command is not configured.

Syntax:

```
CWMP Config$[no] provision-code <string>
```

Example:

```
CWMP Config$provision-code COMPANY-00A026-SAMPLE
```

Command history:

Release	Modification
11.01.02	New command added.

2.2.4 [NO] SESSION

2.2.4.1 SESSION RETRY-LIMIT

Configures the maximum number of retries allowed for each CWMP session fail or connection error. By default, this value is set to 5.

Syntax:

```
CWMP Config$[no] session retry-limit <0...15>
```

Example:

```
CWMP Config$session retry-limit 7
```

Command history:

Release	Modification
11.01.02	New command added.

Chapter 3 Examples

3.1 CWMP basic configuration

Having a basic configuration that allows the CWMP service to be properly enabled requires certain elements.

First of all, it is necessary to have an IP address configured. This address must be the same as the one configured at the local server.

```
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 192.168.1.2 255.255.255.0
;
```

It is also necessary to have a DNS server in order to find the url configured at the CWMP.

```
;
   feature dns
; -- DNS resolver user configuration --
      server 192.168.1.3
   exit
;
```

Then, configure CWMP to enable service.

```
;
   feature cwmp
; -- CPE WAN Management Protocol configuration --
      local user localsample
      local password ciphered 0x1043763EC78425B0AF7346E3684F967B
      local ip-address 192.168.1.2
      management-server user sample-cpe
      management-server password ciphered 0xAD09D54A4C2706AFB3C69AC7101D6FD6
      management-server periodic-interval 30
      management-server url http://cwmp.tr069.com
      provision-code COMPANY-00A026-819/11549
      session retry-limit 4
   exit
;
```

The final configuration looks like this:

```
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 192.168.1.2 255.255.255.0
;;
   feature dns
; -- DNS resolver user configuration --
      server 192.168.1.3
   exit
;
;
   feature cwmp
; -- CPE WAN Management Protocol configuration --
      local user localsample
      local password ciphered 0x1043763EC78425B0AF7346E3684F967B
      local ip-address 192.168.1.2
      management-server user sample-cpe
      management-server password ciphered 0xAD09D54A4C2706AFB3C69AC7101D6FD6
      management-server periodic-interval 30
      management-server url http://cwmp.tr069.com
      provision-code COMPANY-00A026-SAMPLE
      session retry-limit 4
   exit
;
```

3.2 CWMP secured configuration

In order to have a configuration that allows the CWMP service to be properly secured, it is necessary to take more elements into consideration (as shown below).

A valid time must be configured in the device because TLS checks the validity of the certificates. To do this, please configure a valid NTP server.

```
;
   feature ntp
; -- NTP Protocol user configuration --
      protocol
      peer address 1 192.168.1.4
   exit
;
```

Another option is to manually configure the time through the **time set** command. This is not recommended in devices that do not support RTC, since the time has to be set at every reboot.

In order to have a secured connection, a valid CA must be configured. To load a certificate in base64, you can enter the **certificate <certname> base64** command and insert the certificate through the device's ipsec certificate menu. This generates an ipsec configuration, as shown in the example. For further details, please see the section on Certificates (chapter 2) in manual bintec-Dm739-I IPSEC.

```
;
   protocol ip
; -- Internet protocol user configuration --
      ipsec
; -- IPSec user configuration --
         cert
; -- Cert user configuration --
            file b64new COMPANY.CER
            file add "-----BEGIN CERTIFICATE-----"
            file add MIID5TCCAs2gAwIBAgIJAI0yELRu6Sz3MA0GCSqGSIb3DQEBCwUAMIGIMQswCQYD
            file add VQQGEwJFUzEPMA0GA1UECAwGTWFkcmlkMRQwEgYDVQQHDAtUcmVzIENhbnRvczEP
            file add MA0GA1UECgwGVGVsZGF0MQwwCgYDVQQLDANSJkQxETAPBgNVBAMMCENXTVBfQUNT
            file add MSAwHgYJKoZIhvcNAQkBFhFtbHVxdWVAdGVsZGF0LmNvbTAeFw0xNzAxMDIxMjQ3
            file add MDRaFw0xOTEwMjMxMjQ3MDRaMIGIMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTWFk
            file add cmlkMRQwEgYDVQQHDAtUcmVzIENhbnRvczEPMA0GA1UECgwGVGVsZGF0MQwwCgYD
            file add VQQLDANSJkQxETAPBgNVBAMMCENXTVBfQUNTMSAwHgYJKoZIhvcNAQkBFhFtbHVx
            file add dWVAdGVsZGF0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALwt
            file add zuSYVAY+fvQBqrcI5deVzVU2a51SFqsTlehTQ16KPJcoCKE9rxVuxo23+OS3YD8C
            file add 2iRBrVhTDgmZBUuBNaV+yC9pI9zNFHHXfJ241CrY1CXWv6JOPyI5l50Zsbrxvokf
            file add 45FapyXm4gr/L9Ldb21WYh/0SQI71kNCB34H1Pc7eHCR3JaP+WJln54DNCoLefsw
            file add dom4TYVVnoZAencWdV37PhZEdznn5uzSf+mLkUU7voqB9YYTBmud70zwNSdohueg
            file add zI4KK9uhnBdmbNzEItAu2XNM8HosrTWYaZl3l6zRVedZa6f7YA5FFn14VdYCahck
            file add aFPVKqoSlwXakE4leXUCAwEAAaNQME4wHQYDVR0OBBYEFF5n8doD8slZJH0Miirl
            file add 8gTFjvGxMB8GA1UdIwQYMBaAFF5n8doD8slZJH0Miirl8gTFjvGxMAwGA1UdEwQF
            file add MAMBAf8wDQYJKoZIhvcNAQELBQADggEBAJt48X554ESjQ2dpzeuaoZumE8ELfXbB
            file add S03VgVwG3ZZHmkEwObwQ0Eiw0kog96zLIX5Q/gui1m6+v3d2YulPgpnjtwCH+Mi5
            file add CrmRQev/4Kehl5x+cj6KLhkPDhDVZVS97EWhOkG4EPu4pp1BDoZnEHJ1YC5hbM/X
            file add o9XZIRepOCdflOSm5LV98GylRRuHYhS6hrEfP96SHceBadY5LxuF0ZtECCZmehxS
            file add 5W4I3bGLa+cNVPoae8IqlVe79ULWwctG9kNaEHuCvnktWs8aLpTEJpwVpJCUG4CK
            file add qszIzODmz1keABpQAYVUwUoCIa2KTTVJefZ5K2Gq7JLL0d1TSTObtKA=
            file end "-----END CERTIFICATE-----"
;
            certificate COMPANY.CER load
         exit
;
      exit
;
   exit
;
```

Next, configure CWMP to enable service.

```
;
   feature cwmp
; -- CPE WAN Management Protocol configuration --
      local user localsample
      local password ciphered 0x1043763EC78425B0AF7346E3684F967B
      local ip-address 192.168.1.2
      management-server user sample-cpe
      management-server password ciphered 0xAD09D54A4C2706AFB3C69AC7101D6FD6
      management-server periodic-interval 30
      management-server ca cert-name COMPANY.CER
      management-server url https://cwmp.tr069.com
      provision-code COMPANY-00A026-SAMPLE
      session retry-limit 4
   exit
;
```

The final configuration looks like this:

```
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 192.168.1.2 255.255.255.0
;
;
   exit
;
;
;
;
;
   protocol ip
; -- Internet protocol user configuration --
      ipsec
; -- IPSec user configuration --
         cert
; -- Cert user configuration --
            file b64new COMPANY.CER
            file add "-----BEGIN CERTIFICATE-----"
            file add MIID5TCCAs2gAwIBAgIJAI0yELRu6Sz3MA0GCSqGSIb3DQEBCwUAMIGIMQswCQYD
            file add VQQGEwJFUzEPMA0GA1UECAwGTWFkcmlkMRQwEgYDVQQHDAtUcmVzIENhbnRvczEP
            file add MA0GA1UECgwGVGVsZGF0MQwwCgYDVQQLDANSJkQxETAPBgNVBAMMCENXTVBfQUNT
            file add MSAwHgYJKoZIhvcNAQkBFhFtbHVxdWVAdGVsZGF0LmNvbTAeFw0xNzAxMDIxMjQ3
            file add MDRaFw0xOTEwMjMxMjQ3MDRaMIGIMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTWFk
            file add cmlkMRQwEgYDVQQHDAtUcmVzIENhbnRvczEPMA0GA1UECgwGVGVsZGF0MQwwCgYD
            file add VQQLDANSJkQxETAPBgNVBAMMCENXTVBfQUNTMSAwHgYJKoZIhvcNAQkBFhFtbHVx
            file add dWVAdGVsZGF0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALwt
            file add zuSYVAY+fvQBqrcI5deVzVU2a51SFqsTlehTQ16KPJcoCKE9rxVuxo23+OS3YD8C
            file add 2iRBrVhTDgmZBUuBNaV+yC9pI9zNFHHXfJ241CrY1CXWv6JOPyI5l50Zsbrxvokf
            file add 45FapyXm4gr/L9Ldb21WYh/0SQI71kNCB34H1Pc7eHCR3JaP+WJln54DNCoLefsw
            file add dom4TYVVnoZAencWdV37PhZEdznn5uzSf+mLkUU7voqB9YYTBmud70zwNSdohueg
            file add zI4KK9uhnBdmbNzEItAu2XNM8HosrTWYaZl3l6zRVedZa6f7YA5FFn14VdYCahck
            file add aFPVKqoSlwXakE4leXUCAwEAAaNQME4wHQYDVR0OBBYEFF5n8doD8slZJH0Miirl
            file add 8gTFjvGxMB8GA1UdIwQYMBaAFF5n8doD8slZJH0Miirl8gTFjvGxMAwGA1UdEwQF
            file add MAMBAf8wDQYJKoZIhvcNAQELBQADggEBAJt48X554ESjQ2dpzeuaoZumE8ELfXbB
            file add S03VgVwG3ZZHmkEwObwQ0Eiw0kog96zLIX5Q/gui1m6+v3d2YulPgpnjtwCH+Mi5
            file add CrmRQev/4Kehl5x+cj6KLhkPDhDVZVS97EWhOkG4EPu4pp1BDoZnEHJ1YC5hbM/X
            file add o9XZIRepOCdflOSm5LV98GylRRuHYhS6hrEfP96SHceBadY5LxuF0ZtECCZmehxS
            file add 5W4I3bGLa+cNVPoae8IqlVe79ULWwctG9kNaEHuCvnktWs8aLpTEJpwVpJCUG4CK
            file add qszIzODmz1keABpQAYVUwUoCIa2KTTVJefZ5K2Gq7JLL0d1TSTObtKA=
            file end "-----END CERTIFICATE-----"
;
            certificate COMPANY.CER load
         exit
;
      exit
```

```
;
   exit
;
;
;
;
   feature ntp
; -- NTP Protocol user configuration --
      protocol
      peer address 1 192.168.1.4
   exit
;
   feature dns
; -- DNS resolver user configuration --
      server 192.168.1.3
   exit
;
;
   feature cwmp
; -- CPE WAN Management Protocol configuration --
      local user localsample
      local password ciphered 0x1043763EC78425B0AF7346E3684F967B
      local ip-address 192.168.214.59
      management-server user sample-cpe
      management-server password ciphered 0xAD09D54A4C2706AFB3C69AC7101D6FD6
      management-server periodic-interval 30
      management-server ca cert-name COMPANY.CER
      management-server url https://cwmp.tr069.com
      provision-code COMPANY-00A026-SAMPLE
      session retry-limit 4
   exit
;
```

Chapter 4 Annex A

4.1 Third Party Software

When it comes to TLS negotiation, CIT uses the OpenSSL library code.

Please see a copy of the OpenSSL license below:

The OpenSSL toolkit remains under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. The actual license texts can be found below.

OpenSSL License

Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided the following conditions are met:

(1) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

(2) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

(3) All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project to be used in the OpenSSL Toolkit. (http://www.openssl.org/)"

(4) The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. To obtain written permission, please contact openssl-core@openssl.org.

(5) Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without the OpenSSL Project's prior written permission.

(6) Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project to be used in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USAGE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) IN ANY WAY ARISING FROM THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms, save Tim Hudson (tjh@cryptsoft.com) is the holder.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

(1) Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

(2) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

(3) All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographically related.

(4) If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) IN ANY WAY ARISING FROM THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license (including the GNU Public License).