APPENDIX **B**

Server Administration and Configuration

This appendix includes the following information on the administration and configuration of Cisco Prime Optical GateWay/CORBA:

B.1 Creating an OSS Client Profile for GateWay/CORBA

The CORBA gateway authenticates the OSS against a previously created user profile before allowing access to Prime Optical. You can create OSS client profiles for GateWay/CORBA sessions. Each OSS profile defines GateWay/CORBA parameters, such as the OSS profile name, password, and IP address.

OSS client profiles are stored in the GateWay/CORBA Users table.

Step 1 Log into the Cisco Prime Optical client with administrator privileges.

Step 2 In the Domain Explorer window, choose **Administration > GW/CORBA Users**.

Step 3 Choose **Edit > Add** (or click the **Create a New User** tool).

Step 4 In the Add GW/CORBA User window, enter the following OSS client information:

- OSS Profile Name—Name of the OSS profile.
- Password—Password that the OSS client uses to log into the Prime Optical server. The password must contain at least one special character, at least two alphabetic characters (A-Z, a-z), and at least one numeric character (0-9). Apostrophes (‘) are not accepted.
- Confirm Password—Re-enter the password to confirm it.

Step 5 Click **OK** to confirm the information. Changes take effect immediately. The GW/CORBA Users table receives a refresh event. If automatic refresh is enabled, the new OSS client profile appears as a new row in the table. If automatic refresh is disabled, click the **Refresh Data** tool to see the new OSS client profile in the table.

Step 6 In the Control Panel window, choose **Administration > GW/CORBA Users**. The GW/CORBA Users wizard displays a profile for each OSS client that uses a GateWay/CORBA service.

B.2 Deleting an OSS Client Profile for GateWay/CORBA

Step 1 Log into the Prime Optical client with administrator privileges.

Step 2 In the Domain Explorer window, choose **Administration > GW/CORBA Users**.

Step 3 The GW/CORBA Users table displays a list of available OSS users. Select the OSS user to delete.

Step 4 Choose **Edit > Delete** (or click the **Delete a User** tool) to delete the OSS profile from the Prime Optical database.

Step 5 Click **OK** to confirm the deletion. The OSS client profile name is deleted from the GW/CORBA Users table.

Note If the OSS is connected to Prime Optical when the profile is being deleted, Prime Optical does not terminate the OSS session.

B.3 Viewing Currently Logged In GateWay/CORBA OSS Users

Step 1 Log into the Prime Optical client with administrator privileges.

Step 2 In the Domain Explorer window, choose **Administration > GW/CORBA Users**

Step 3 The GW/CORBA Users table displays a list of available OSS users. Click the **Show Logged in GW CORBA Users** tool.

Step 4 In the Active GW/CORBA Users table, a list of currently logged-in users is displayed, including the OSS profile name, IP address to which the user is logged in, and the login time.

B.4 Logging Out GateWay/CORBA OSS Users

Step 1 Log into the Prime Optical client with administrator privileges.

Step 2 In the Domain Explorer window, choose **Administration > GW/CORBA Users**.

Step 3 The GW/CORBA Users table displays a list of available OSS users. Click the **Show Logged in GW CORBA Users** tool.

Step 4 In the Active GW/CORBA Users table, a list of currently logged-in users is displayed, including the OSS profile name, IP address to which the user is logged in, and the login time. Select the user to log off.

Step 5 Click the **Log Out GW CORBA User** tool.

Step 6 The user session is cleared from the Active GW/CORBA Users table. You will notice the loss of session during the next ping cycle or when you try to perform an operation on another manager. Some examples of user operations are:

- The user is connected and performs a query operation on the EMS. The OSS user starts to query the EMS by getting a fresh object reference from the manager through an emsSession query. Because the session has been cleared by the GateWay/CORBA service, the OSS user receives an exception and notices the loss of session.
- The Prime Optical client forcefully logs out the user. The OSS user does not immediately notice the loss of session when the Prime Optical client forces a logout. To immediately log out the user, the GateWay/CORBA service makes a call to the NMS session interface, which forces the OSS client applications to modify their shutdown application. This is not the preferred method.
- The GateWay/CORBA service clears the user session information from its internal memory and database.

B.5 Unsupported Events

The Events with INDETERMINATE severity that are reported in the Alarm Log Browser of the Managed Element in Cisco Prime Optical are not moved to the external OSS clients through the CORBA Gateway.

Note The severity of the Performance Monitoring Threshold Crossing Alerts (TCAs) are always set to INDETERMINATE and are moved to the external OSS Client. For more information, see A.4.6 Threshold Crossing Alert, page A-9.

B.6 Using Encryption Between the OSS Client and GateWay/CORBA

Prime Optical uses improved encryption of usernames and passwords for network security. You can set the Control Panel to send encrypted usernames and passwords to GateWay/CORBA:

Step 1 Log into the Prime Optical client with administrator privileges.

Step 2 In the Domain Explorer window, choose **Administration > Control Panel**.

Step 3 Click the **GateWay/CORBA Service** tab for the GateWay/CORBA Service property sheet.

Step 4 Click the **Global** tab and check the **Enable Encryption for Username and Password check** box.

Step 5 Click **Save**; then, click **Yes** in the confirmation dialog box. Changes take effect immediately.

If the OSS clients enable the encryption feature, they must provide implementation for RSA-based encryption by retrieving the RSA public key or the public key pair from GateWay/CORBA and by using cryptographic libraries.

- To obtain the RSA public key from Prime Optical, use the emsSessionFactory::EmsSessionFactory_I:: getEmsPublicKey API. See 3.5.2 getEmsPublicKey, page 3-53.
- To obtain the RSA public key pair from Prime Optical, use the emsSessionFactory::EmsSessionFactory_I:: getEmsPublicKeyPair API. See 3.5.3 getEmsPublicKeyPair, page 3-54.

Prime Optical uses a 512-bit (64-byte) key size and returns the string representation of the RSA public key or public key pair, encoded in the Base64 encoding scheme. OSS clients should use Base64 decoders to decode the public key and get the byte[] of the public key from the decoded public key string. The byte[] corresponding to the public key represents the key in its primary encoded format (X.509 SubjectPublicKeyInfo). Using this byte[] and cryptographic libraries, the RSA public key can be created.

One example of the security provider is Bouncy Castle Provider.

Use the public key to encrypt the username and password. Before passing the encrypted username and password to Prime Optical for login, OSS clients should encode the encrypted username and password by using Base64 encoders to obtain the string equivalent of the encrypted data.

Note Use cryptographic libraries implementing RSA public key encryption supporting the “PKCS #1 v2.0 EME-PKCS1-v1_5 (PKCS #1 v1.5 block type 2), PKCS1Padding” encoding scheme. Prime Optical does not provide these cryptographic libraries.

B.7 Using Multiple Naming Servers

Prime Optical can register with multiple naming servers. You must add the following parameters to the *Prime Optical-server-installation-directory*/cfg/corbagw.properties file:

- corbagw.namingservice.ServerList=ctmc4-u80,ctm7-u60
- corbagw.namingservice.RootIORLoc=/namingroot.ior

Complete the following steps to allow Prime Optical to use multiple naming servers:

Step 1 In the Domain Explorer window, choose **Administration > Control Panel**.

Step 2 Click **GateWay/CORBA Service** to open the GateWay/CORBA Service pane.

Step 3 In the **Global** tab > **GateWay/CORBA Configuration** area, specify the following parameters:

- Name Service Server List—Lists all the hosts on which the naming service is running. The hosts should be reachable from the Prime Optical server host, and the HTTP server must be running on all naming service hosts. Enter **ctmc4-u80, ctm7-u60**.

Note In addition to these naming service hosts, Prime Optical registers itself with the local naming service. The local naming service port is 14005 and is bundled with Prime Optical.

- Name Service Root IOR—Defines the location and name of the file that contains the naming service root Interoperable Object Reference (IOR). The IOR file must be accessible through the following HTTP call: http://*name-server-IP-address*:80/namingroot.ior. Enter **/namingroot.ior**.

Step 4 Restart the GateWay/CORBA service.

B.8 Naming Conventions for Published GateWay/CORBA Objects

GateWay/CORBA publishes two top-level objects: EMSSessionFactory and NotificationChannel. Prime Optical creates these objects and registers them with the CORBA name server.

GateWay/CORBA creates naming contexts under the root as shown in Figure B-1. The last context in the tree must have a different name. To change this value in the Prime Optical client GUI:

Step 1 Log into the Prime Optical client with the appropriate Prime Optical user access profile.

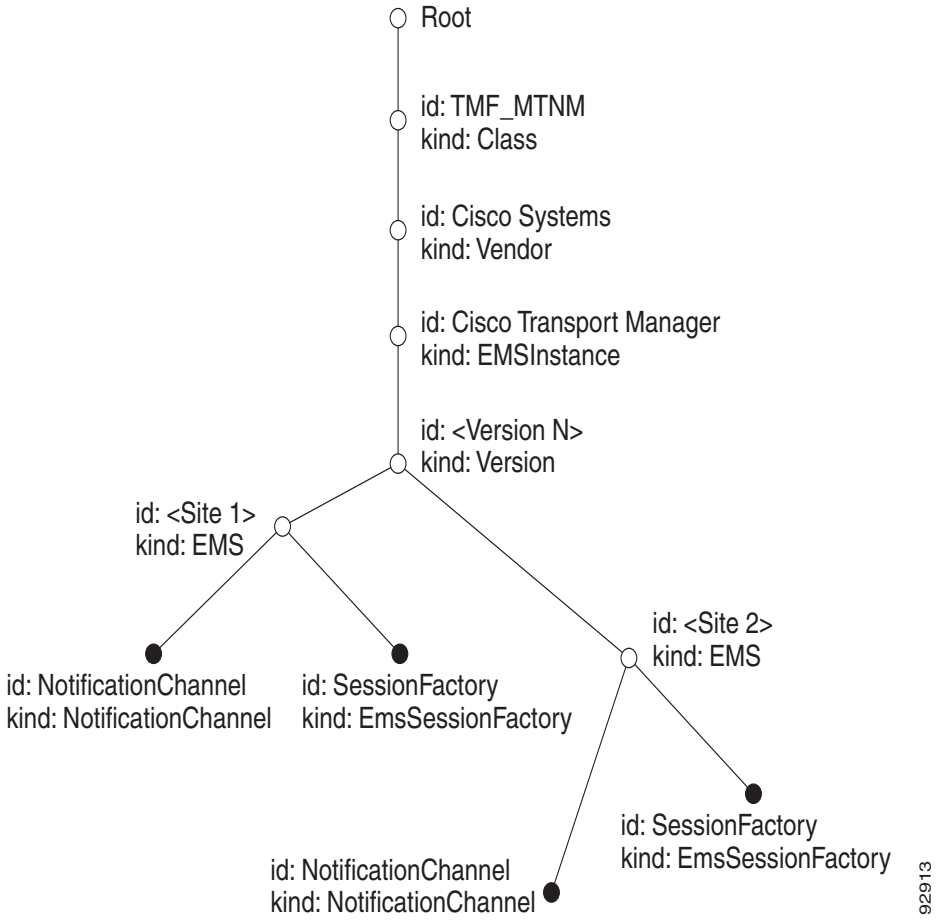
Step 2 In the Domain Explorer window, click the **Domain** node.

Step 3 In the Management Domain Properties sheet, click the **Identification** tab.

Step 4 In the EMS Domain section, look for **EMS ID**. The value of this field should be used as the “id” field for context, where “kind” equals “EMS.” The default value is *CTM*. By using different names, you can install multiple instances of Prime Optical and use a centralized naming server and repository.

The following figure shows the naming scheme for GateWay/CORBA objects.

Figure B-1 Naming Scheme for GateWay/CORBA Objects



B.9 Location of the Naming Service IOR File

The naming service IOR is located at:

/opt/CiscoTransportManagerServer/openfusion/domains/OpenFusion/localhost/NameService/NameSingleton/NameSingleton.ior

B.10 Useful Debugging Utilities for Resolving Naming Service-Related Issues

The following are samples of Prime Optical commands (bundled utility programs) for debugging naming service connectivity issues.

Obtain the list of registered objects in the OpenFusion naming service:

```
setenv PATH /opt/CiscoTransportManagerServer/openfusion/bin:$PATH
```

```
setenv NS_IOR_LOCATION
file:///opt/CiscoTransportManagerServer/openfusion/domains/OpenFusion/localhost/NameServic
e/NameSingleton/NameSingleton.ior
nsMgrTool -l
```

Decode an IOR file:

```
setenv PATH /opt/CiscoTransportManagerServer/openfusion/bin:$PATH
dior -f <IOR file name>, or
dior -i <IOR string>
```

Check if the naming service is running:

```
setenv PATH /opt/CiscoTransportManagerServer/openfusion/bin:$PATH
server -status NameService
```

Note The /opt/CiscoTransportManagerServer/openfusion/bin directory contains nsMgrTool, dior, and server utility tools.

B.11 Configuring GateWay/CORBA

You can configure the following GateWay/CORBA properties in the Prime Optical client Control Panel.

Step 1 From the Domain Explorer, choose **Administration > Control Panel**.

Step 2 In the Control Panel, click **GateWay/CORBA Service**. Configure the following properties:

Note If GateWay/CORBA is running, changes to the config file do not take effect dynamically. You must restart GateWay/CORBA for the changes to take effect.

- Enable Encryption for username and password:

  This property defines whether to encrypt the username and password used for the GateWay/CORBA client.

- Heartbeat for Notification Channel (min): 0

  This property is the rate at which the notification service is checked. A zero entry means not to check the notification service.

- Enter the maximum number of simultaneous sessions: 4

  This property is the number of GateWay/CORBA sessions that can be active at the same time. The range is from 4 to 25 sessions.

- Enter the maximum events per consumer: 10000

  GateWay/CORBA uses this property to set the MaxEventsPerConsumer administrative QoS parameter of the notification channel. The notification server uses this property to bound the maximum number of events in a given channel that are allowed to queue at any given time. The default value is 0, where the notification server does not impose a limit on the maximum number of events that can be queued. If no limits are imposed on the queue, the notification server might run out of memory if a client behaves incorrectly. The server must keep all events in memory until they are consumed by all registered consumers.

Caution Any change to this value should be made with extreme caution. If you set the value too low, the NMS will not receive all notifications. If you set the value too high, the Prime Optical notification server will run out of memory. The current value is set to handle alarm bursts of 10,000 events per minute.

- Enter the notification service name: NotificationService

  This property defines the service name that the resolve_initial_reference function uses to get a reference to the notification service. The GateWay/CORBA installation installs the notification service automatically. To use your own notification service, modify this parameter.

Tip You do not need to change this parameter if you plan to use the notification service that is bundled with GateWay/CORBA.

- Enter the notification service naming context: services/NotifyChannelFactory

  NamingContext defines the naming context of NotificationService. This property is used when resolve_initial_reference fails to resolve NotificationService. GateWay/CORBA contacts the naming service to resolve the name context defined in this property. The value of this property must match the value published by your notification server.

Tip You do not need to change this parameter if you plan to use the notification service that is bundled with GateWay/CORBA.

- Enter the notification service factory IOR filename: file:/opt/CiscoTransportManagerServer/openfusion/domains/OpenFusion/localhost/NotificationService/NotificationSingleton/NotificationSingleton.ior

  The FactoryIORFile property defines the path to a text file that contains the IOR of NotificationService. This property is used only after resolve_initial_reference and naming service fail. GateWay/CORBA opens the file as defined by the URL format in this property and attempts to retrieve the IOR from this file. This parameter lets you run your notification service on a different host to improve performance.

Tip You do not need to change this parameter if you plan to use the notification service that is bundled with GateWay/CORBA.

- Enter the notification service listening port number: 0

  This property is used to set the port that the notification service uses to listen for incoming requests. The port number is set in the IOR for the notification service. The use IOR and use IOR endpoint properties are set correctly. The default port number is zero, which signifies the port number allocated by the operating system.

- Enter the session port number: 0

  This property configures the EMSSessionFactory port. If this property is set to zero, the operating system allocates the session port number.

- Enter the name service server list:

This property defines where the name servers are running. This property accepts a comma-separated list of hostnames.

- Enter the name service root IOR:

  This property defines the path used to find the naming service IOR on each host defined in ServerList. The complete path is constructed as http://*item-of-ServerListRootIORLoc*

- Error level: Minor

  This property defines the error level of messages to log.

  You can configure this GateWay/CORBA property by modifying a configuration file in *Prime Optical-server-installation-directory*/cfg/corbagw.properties.

- corbagw.CTP.getLayeredParameters=false

  By default, this property is not enabled. If the NMS requires CTP-related transmission parameters to be included as part of an object reporting TerminationPoint_T structure, this property must be set to true. However, the ManagedElementMgr_I.getTP interface always returns transmission parameters as part of the TerminationPoint_T structure and is independent of this property setting.

B.12 Using the CLI to Start and Stop GateWay/CORBA

Prime Optical can manage the GateWay/CORBA service from the command line:

- To start a GateWay/CORBA service, run the /opt/CiscoTransportManagerServer/bin/gwcorba-start script from the command line.
- To stop a GateWay/CORBA service, run the /opt/CiscoTransportManagerServer/bin/gwcorba-stop script from the command line.

Only Prime Optical users with administrative privileges can run these scripts. If the GateWay/CORBA service is already running and you attempt to run the gw-start script, the script exits with the message "GWCORBA already running." If the GateWay/CORBA service is stopped and you attempt to run the gw-stop script, the script exits with the message "GWCORBA not running."

You must have a Prime Optical username and password with a SysAdmin or SuperUser profile to start or stop the scripts.

B.13 Configuring Secure Socket Layer for GateWay/CORBA

To ensure network security, CORBA calls can be made over Secure Socket Layer (SSL).

The current JacORB implementation is precompiled with JacORB security libraries. To configure SSL for GateWay/CORBA, you must set up a keystore and configure the properties in the client-side jacorb.properties file.

The client must enforce SSL by modifying the jacorb.properties file. The server-side keystore is generated using the JSSE keystore. Prime Optical bundles a default keystore and a certificate for the GateWay/CORBA service.

As explained in the following sections, you must generate the server-side certificate and add it to the client-side keystore; then generate and add the client-side certificate to the server-side keystore.

B.13.1 Generating the Server-Side Certificate

Step 1 Enter the **keytool** command to generate a keystore and a key:

```
keytool -genkey -alias gwcorba_service -validity 25000 -keystore gwcorba_service_ks
-storepass gwcorba_service_ks_pass -keypass gwcorba_service_ks_pass

What is your first and last name?
  [Unknown]:  gateway corba server
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:  cisco
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is <CN=gateway corba server, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown>
correct?
  [no]:  y
```

Step 2 Verify that the generated keystore and key have the following attributes:

```
Keystore name: gwcorba_service_ks
Alias: gwcorba_service
Keystore password: gwcorba_service_ks_pass
Key password: gwcorba_service_ks_pass
Validity: 25000 days
```

Step 3 Enter the following command to generate a server-side certificate that will be issued to the client:

```
keytool -export -keystore gwcorba_service_ks -alias gwcorba_service -storepass
gwcorba_service_ks_pass -file gwcorba_service_cert

Certificate stored in file <gwcorba_service_cert>
```

Step 4 Verify that the certificate is stored in the gwcorba_service_cert file. The server-side certificate and keystore are present in the /opt/CiscoTransportManagerServer/cfg directory.

B.13.2 Generating the Client-Side Certificate

Note the following conventions:

- ascii_client_ks—Denotes a client-side keystore.
- ascii_client_cert—Denotes a client-side certificate.
- gwcorba_service_ks—Denotes a server-side keystore.
- gwcorba_service_cert—Denotes a server-side certificate.

Step 1 Enter the **keytool** command to generate a keystore:

```
keytool -genkey -alias ascii_client -validity 25000 -keystore ascii_client_ks -storepass
ascii_client_ks_pass -keypass ascii_client_ks_pass

What is your first and last name?
```

```
  [Unknown]:  ascii client
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:  cisco
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=ascii client, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown correct?
[no]:  y
```

Step 2 Verify that the generated keystore and key have the following attributes:

```
Keystore name: ascii_client_ks
Alias: ascii_client
Keystore password: ascii_client_ks_pass
Key password: ascii_client_ks_pass
Validity: 25000 days
```

Step 3 Enter the following command to generate a client-side certificate that will be issued to the server:

```
keytool -export -keystore ascii_client_ks -alias ascii_client -storepass
ascii_client_ks_pass -file ascii_client_cert

Certificate stored in file <ascii_client_cert>
```

Step 4 Verify that the certificate is stored in the ascii_client_cert file.

B.13.3 Adding the Client-Side Certificate to the Server-Side Keystore

Step 1 Enter the following command to add the client-side certificate to the server-side keystore. (Use FTP or a similar tool to deliver the ascii_client_cert file to the server. The server-side keystore is located in the /opt/CiscoTransportManagerServer/cfg directory on the server.)

```
keytool -import -keystore gwcorba_service_ks -alias ascii_client -storepass
gwcorba_service_ks_pass -file ascii_client_cert
```

The command output resembles the following example:

```
Owner: CN=ascii client, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Issuer: CN=ascii client, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Serial number: serial-number
Valid from: Sat Mar 18 17:18:44 GMT+05:30 2008 until: Fri Jul 23 10:50:28 GMT+05:30 2038
Certificate fingerprints:
    MD5: 42:53:98:7C:BA:CB:28:39:50:50:9F:E4:56:F2:43:FF
    SHA1: F5:1D:B9:BB:1D:66:C2:A1:32:BE:47:0C:85:47:17:16:A2:69:17:4C
Trust this certificate? [no]: y
Certificate was added to keystore
```

Step 2 Verify that the certificate issued by the client was added to the server keystore.

B.13.4 Adding the Server-Side Certificate to the Client-Side Keystore

Step 1 Enter the following command to add the server-side certificate to the client-side keystore. (Use FTP or a similar tool to deliver the previously generated gwcorba_service_cert file from the server. The server-side certificate is located in the /opt/CiscoTransportManagerServer/cfg directory on the server.)

```
keytool -import -keystore ascii_client_ks -alias gwcorba_service -storepass
ascii_client_ks_pass -file gwcorba_service_cert
```

The command output resembles the following example:

```
Owner: CN=gateway corba server, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Issuer: CN=gateway corba server, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Serial number: serial-number
Valid from: Sat Mar 18 17:21:24 GMT+05:30 2008 until: Fri Jul 23 10:53:08 GMT+05:30 2038
Certificate fingerprints:
    MD5: 5C:41:39:AD:D0:F8:63:5D:81:8D:47:A0:33:02:8E:7D
    SHA1: 38:CD:C8:57:F7:15:22:DC:1A:6E:99:CD:13:A1:9A:67:90:2C:65:C2
Trust this certificate? [no]: y
Certificate was added to keystore
```

Step 2 Verify that the certificate issued by the server was added to the client keystore.

B.13.5 Configuring the Client-Side Properties

To enforce SSL, complete the following configuration on the client-side jacorb.properties file.

Note

- To enforce SSL, the supported and required options must be set to 60.
- No changes are required to the server-side jacorb.properties file, because it has already been changed.

```
jacorb.security.support_ssl=on

# IIOP/SSL parameters (numbers are decimal values):
# EstablishTrustInClient = 40
# EstablishTrustInTarget = 20
# mutual authentication = 60
jacorb.security.ssl.client.supported_options=60
jacorb.security.ssl.client.required_options=60

jacorb.ssl.socket_factory=org.jacorb.security.ssl.sun_jsse.SSLSocketFactory

jacorb.security.keystore_password= ascii_client_ks_pass
jacorb.security.keystore= ascii_client_ks

# Read trusted certificates from the keystore
jacorb.security.jsse.trustees_from_ks=on
```

B.14 Installation Program

The Prime Optical installation program installs the GateWay/CORBA component, which includes OpenFusion 4.2.3 (JacORB, Notification Service, and Name Service) from Prism Technologies.

Interface Definition Language (IDL) files are installed under the /opt/CiscoTransportManagerServer/idl directory. See the *Cisco Prime Optical 9.3.1 Installation Guide* for more information.

B.15 Cisco Prime Optical 9.3-to-Cisco Prime Optical 9.3.1 Migration

All procedures related to the migration from Cisco Prime Optical 9.3 to Cisco Prime Optical 9.3.1 are performed during the installation phase; no additional operations are required.