



APPENDIX **E**

Configuring Prime Performance Manager to Run with Various Networking Options

In addition to running on standard IP-connected networks, the Cisco Prime Performance Manager has the flexibility to adapt to a variety of different networking environments, including firewall and Secure Sockets Layer (SSL). Prime Performance Manager software can run in each of these environments individually, or in any combination of networking environments.

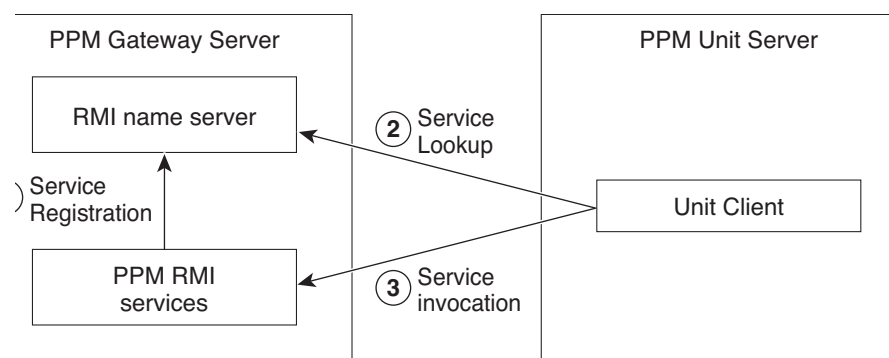
This appendix describes communication between Prime Performance Manager Gateway and Prime Performance Manager Unit servers and between the Prime Performance Manager Gateway and web based clients. [Figure E-1](#) includes the following:

- Two-way Remote Method Invocation (RMI) communication between Gateway and Unit server processes. The server processes can send requests to and receive responses from the each other. Each of them can send unsolicited notifications to the other.

For example, if a Unit detects that a Node's state has changed, it sends a notification to the Gateway to update its Database.

- One-way HTTP communication between a web browser and a Prime Performance Manager Gateway embedded web server, using the request/response model.

Figure E-1 Prime Performance Manager Communication



This appendix contains:

- [How Does RMI Work?](#), page E-2
- [Firewall Communication](#), page E-3

How Does RMI Work?

Remote Method Invocation (RMI) is a Java-based technology that allows a Java application to communicate with another Java application (usually residing on different hosts) using remote method invocation.

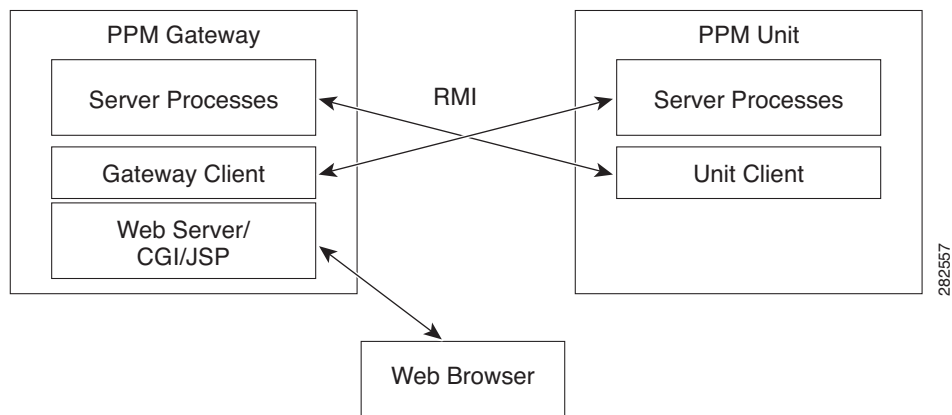
RMI marshals and unmarshals method parameters and return values using Java object serialization. It uses TCP connections as the default communication mechanism.

If you know how RMI works, you can understand the different scenarios in this appendix.

The types of RMI components that exist between Prime Performance Manager client and server communication are:

- **RMI name server**—Runs on Prime Performance Manager Gateway and Unit servers.
- **Prime Performance Manager RMI services**—Runs on Prime Performance Manager Gateway and Unit servers.
- **Prime Performance Manager client process**—Run on Prime Performance Manager Gateway and Unit servers.

Figure E-2 RMI Components



When Prime Performance Manager Server starts, Prime Performance Manager RMI services register with the RMI name server. These registered RMI services have one single published IP address.

When Prime Performance Manager Client starts, it first establishes a TCP connection to the RMI name server and performs a service lookup.

The RMI name server returns the published IP address for Prime Performance Manager RMI services. Prime Performance Manager Client then establishes another TCP connection to the published IP address of Prime Performance Manager RMI services for client and server communication.

Firewall Communication

To enable Prime Performance Manager client/server communication through a firewall, you need to set up the firewall so that it allows Prime Performance Manager communication packets to pass through freely.

This section contains:

- [Configuring Port Numbers and Parameters, page E-3](#)
- [Configuring Firewalls, page E-3](#)

Configuring Port Numbers and Parameters

The port numbers used by Prime Performance Manager software is configured in the System.properties file:

**Note**

Prime Performance Manager gateway and unit servers communicate using TCP sockets. All port numbers in this section are TCP ports.

- If you installed Prime Performance Manager software in the default directory, /opt, then the location of the file is /opt/CSCOppm-gw/properties/System.properties or /opt/CSCOppm-unit/properties/System.properties
- If you installed Prime Performance Manager software in a different directory, then the file resides in that directory.

Configuring Firewalls

Prime Performance Manager software uses four TCP port numbers on the server side and two TCP port numbers on the client side to communicate between Prime Performance Manager server and client(s).

Step 1 Identify the TCP port numbers that you want to use between Prime Performance Manager gateway and unit and web interface applications.

These ports include the RMI Registry Port, the Data Server Port, the Login Server Port, the Client Port, and the HTTP Web Server port. They are used for two way TCP connections between Prime Performance Manager server and client.

Step 2 Modify the System.properties file on Prime Performance Manager gateway and unit servers.

The System.properties file resides on Prime Performance Manager server under the /opt/CSCOppm-gw/properties or /opt/CSCOppm-unit/properties directory.

If you installed Prime Performance Manager software in a location other than the default (/opt), then specify the path to the file system where you installed the Prime Performance Manager software instead of the default (/opt) path.

Step 3 Using a text editor, edit this file and specify the appropriate port number where indicated subsequently:

**Caution**

Before editing, always make a backup of the file. This ensures a valid file exists in case you make an error while editing.

Step 4 Modify the node configuration files with the selected port numbers.

On Cisco nodes, you can use extended access lists to allow the chosen TCP port numbers to pass between the appropriate interface(s). Assuming a single node separates Prime Performance Manager gateway and unit servers, you can use the following extended access list:



Note

The established entries are necessary, as they allow data to flow between the gateway and unit that initiated the session. Without this keyword, units will not have access to Prime Performance Manager gateway server.

Prime Performance Manager unit Interface:

- Interface FastEthernet 1/1
- ip address 192.168.1.100 255.255.255.0
- ip access-group unit-to-gateway in

Prime Performance Manager gateway Interface:

- interface FastEthernet 2/1
- ip address 192.168.2.100 255.255.255.0
- ip access-group gateway-to-unit in

Access list from unit to gateway contains:

- ip access-list extended unit-to-gateway
- 10 permit tcp any established
- 20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 45742
- 30 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 45751
- 40 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 45752
- 50 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 4440

Access list from gateway to unit contains:

- ip access list extended gateway-to-unit
- 10 permit tcp any established
- 20 permit tcp host 192.168.2.2 192.168.1.0 0.0.0.255 eq 46173

Step 5 Restart Prime Performance Manager server to use the newly chosen TCP port numbers.

As the root user, on Prime Performance Manager server, type:

```
#cd /opt/CSCOppm-gw/bin
#./ppm restart
```

The server processes restart using the newly chosen port numbers.

Both of these access lists allow established TCP connections (10 permit tcp any established, see previous).

When Prime Performance Manager client or server establishes a TCP connection to the other end, it uses a fixed destination port. However, the source port from the initiating party is random. The established keyword allows a returning TCP packet to go back to the random initiating source port.