APPENDIX H

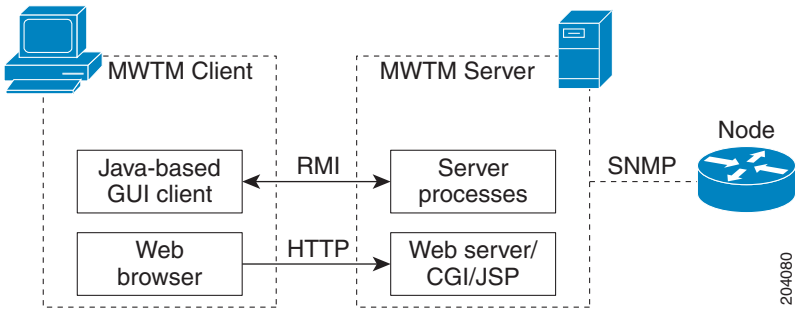
Configuring MWTM to Run with Various Networking Options

In addition to running on standard IP-connected networks, the Cisco Mobile Wireless Transport Manager (MWTM) has the flexibility to adapt to a variety of different networking environments, including Virtual Private Network (VPN), Network Address Translation (NAT), firewall, port-forwarding, and Secure Sockets Layer (SSL). The MWTM software can run in each of these environments individually, or in any combination of networking environments.

This appendix describes communication between the MWTM client and the MWTM server. Figure H-1 includes the following:

- Two-way Remote Method Invocation (RMI) communication between a Java-based GUI client and Java-based server processes. The client can send requests to and receive responses from the server, and the server can send unsolicited notifications to the client. For example, if the server detects that an ITP's state has changed, it sends a notification to all MWTM clients to update their topology windows.
- One-way HTTP communication between a web browser and an MWTM-embedded web server, using the request/response model.

Figure H-1 MWTM Communication



Note This appendix does not address communication between the MWTM server and the ITP, which uses the SNMP protocol for network management.

This appendix contains:

How Does RMI Work?

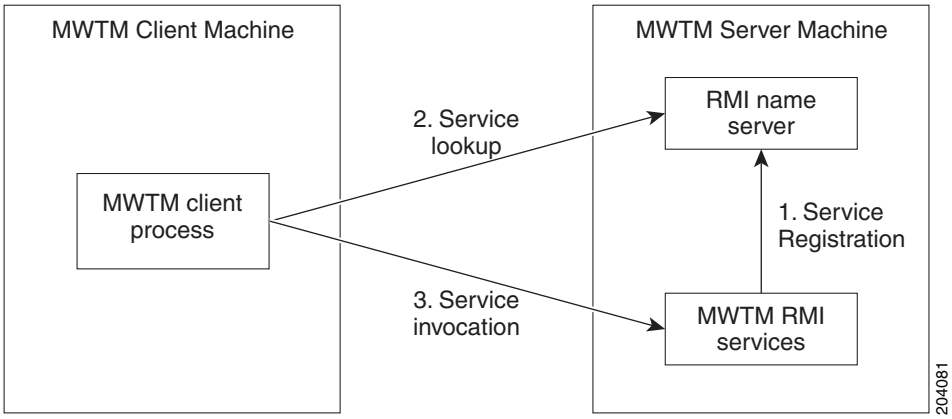
RMI is a Java-based technology that allows a Java application to communicate with another Java application (usually residing on different hosts) using remote method invocation. RMI marshals and unmarshals method parameters and return values using Java object serialization. It uses TCP connections as the default communication mechanism.

Understanding how RMI works can assist your understanding of the different scenarios presented in this appendix.

The types of RMI components that exist between the MWTM client and server communication are:

- **RMI name server**—Runs on the MWTM server
- **MWTM RMI services**—Runs on the MWTM server
- **MWTM client process**—Runs on the MWTM client

Figure H-2 RMI Components



When the MWTM server starts, the MWTM RMI services register with the RMI name server. These registered RMI services have one single published IP address.

When the MWTM 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 the MWTM RMI services. The MWTM client then establishes another TCP connection to the published IP address of the MWTM RMI services for client and server communication.

This appendix describes how to configure the MWTM software to adjust the communication process outlined previously, in order to make the MWTM work with NAT, Port-Forwarding, and/or a Dual-Interface MWTM server.

VPN Communication

Note VPN configuration is transparent to the user; no manual configuration is needed.

MWTM client/server communication can run transparently through a VPN tunnel, which is a secure IP layer, without any user intervention. You can use VPN to connect to a corporate network, then start the MWTM client to connect through the VPN tunnel to an MWTM server in the corporate network.

When the client host establishes a VPN tunnel, the operating system (or system library) sees this as another virtual IP interface. The VPN tunnel does not affect HTTP communication between the web browser and server, it only affects RMI communication between the MWTM client and server processes.

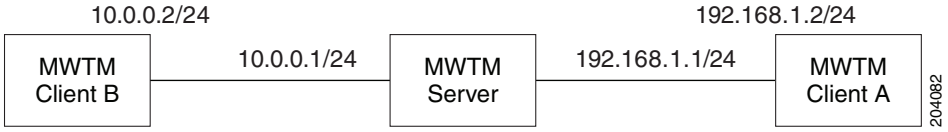
For HTTP communication, the virtual IP address is transparent to the upper layer. The operating system automatically chooses the correct IP address to send out the request packet. For RMI communication, the MWTM client must register with the MWTM server using the correct IP address, so that the server can invoke RMI callbacks and send unsolicited notifications to the client.

The MWTM software solves this problem by automatically detecting the local IP interface so that the MWTM server can send unsolicited notification to the correct IP address.

Figure H-3 shows a sample VPN network with these characteristics:

- The MWTM client with IP address 192.168.0.1 is connected to the MWTM server network through a VPN tunnel.
- The MWTM client host has obtained VPN IP address 10.1.1.2, which is a virtual IP interface.

Figure H-3 VPN Communication



When connecting to the MWTM server, the MWTM client automatically recognizes its VPN IP address, 10.1.1.2, and uses that address to register with the MWTM server to receive RMI callbacks.

NAT Communication

MWTM client/server communication can run through one or more static NAT-connected networks.

Note The MWTM software does not support dynamic NAT or dynamic NAT pool overloading.

In a static NAT network, the MWTM client and server reside on different sides of the NAT network, with no routes between the client network and the server network. The NAT device statically maps the client IP address to a NAT address in the server network, and the server IP address to a NAT address in the client network.

The NAT device translates packets between the MWTM client and server by replacing IP address headers when packets pass through. From the client's point of view, the server appears to be at a NAT IP address in the client network, and vice versa. For most protocols, this technique is sufficient to enable the client and server to communicate.

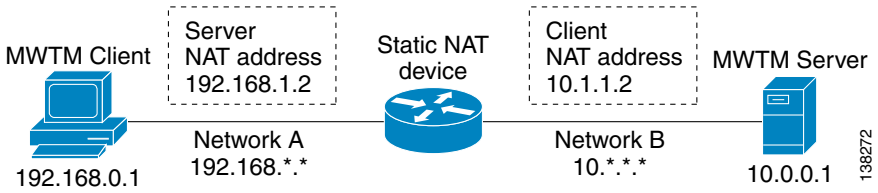
However, for the RMI protocol, this is not sufficient. The RMI protocol requires the client and server to keep remote object references by remote stubs. These remote stubs contain the remote objects' IP addresses, and are passed between the client and server using Java serialization. The NAT device only converts the IP addresses in the IP packet header, but the remote stub object is in the packet content. Therefore, the NAT device cannot recognize the IP address inside the packet, and fails to route it correctly.

The MWTM software solves this problem by creating a specialized NAT-aware socket factory. The user must perform some manual configuration to enable the MWTM to “know” the network NAT configuration.

Figure H-4 shows a sample static NAT network with these characteristics:

- A static NAT device connects Network A (192.168.*.*) to Network B (10.*.*.*), with no routes between Network A and Network B.
- The NAT device maps the MWTM client IP address 192.168.0.1 in Network A to 10.1.1.2 in Network B.
- The NAT device maps the MWTM server IP address 10.0.0.1 in Network B to 192.168.1.2 in Network A.

Figure H-4 Static NAT Communication



To configure the MWTM software in this static NAT network, you must change the MWTM client's *RMIOverNAT.properties* file.

- In Solaris/Linux, if you installed the MWTM software in the default directory, */opt*, then the location of the file is */opt/CSCOsgmClient/properties/RMIOverNAT.properties*.
- In Windows, if you installed the MWTM software in the default directory, *C:\Program Files*, then the location of the file is *C:\Program Files\SGMClient\properties\RMIOverNAT.properties*.
- If you installed the MWTM software in a different directory, then the file resides in that directory.

For the example shown in Figure H-4, you must add this line to the file:

10.0.0.1 = 192.168.1.2

This line maps the MWTM server's real IP address, 10.0.0.1 in Network B, to its NAT address, 192.168.1.2, in Network A, which is the server's IP address as seen by the client.

Note The MWTM server automatically detects the MWTM client's NAT address. No manual configuration on the part of the user is needed at the server side.

When the MWTM server starts, it starts MWTM services that register with the RMI server and publish themselves with the IP address specified in the SERVER_NAME property of *System.properties* file on the MWTM server. In the given example, the published IP address is 10.0.0.1.

The MWTM client starts and connects to 192.168.1.2 (specified as the MWTM client's default server address). The NAT device translates the MWTM client's request to the RMI server at 10.0.0.1.

The MWTM client then asks where the MWTM services are located. The RMI server replies that these MWTM services reside at 10.0.0.1. Without the *RMIOverNAT.properties* file on the MWTM client, the client will try to connect to 10.0.0.1, which would fail.

If we have configured the *RMIOverNAT.properties* file on the MWTM client as in the example, the MWTM client will still connect to 192.168.1.2 for name lookup, and the name server will return that MWTM services are running on 10.0.0.1. The MWTM client then looks in the *RMIOverNAT.properties* file, and discovers that the translated address for 10.0.0.1 is 192.168.1.2. With this configuration, the MWTM client will try to connect to 192.168.1.2 for RMI services (instead of 10.0.0.1). As the result, the connection will be established successfully.

Firewall Communication

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

This section contains:

Configuring Port Numbers and Parameters

Note The MWTM client and server communicate using TCP sockets. All port numbers in this section are TCP ports.

The port number used by the MWTM software is configured in the *System.properties* file:

- If you installed the MWTM software in the default directory, */opt*, then the location of the file is */opt/CSCOsgm/properties/System.properties*.
- If you installed the MWTM software in a different directory, then the file resides in that directory.

Set these parameters on the *server* side of the file:

RMIREGISTRY_PORT = 44742

DATASERVER_PORT = 0

LOGINSERVER_PORT = 0

WEB_PORT = 1774

where:

- RMIREGISTRY_PORT is the port on which the RMI naming server listens. You must specify a port number; **0** is not allowed.
- DATASERVER_PORT is the port on which the Data Service listens. If you specify **0**, the MWTM software uses a random available port, 1024 and above. The MWTM maintains the chosen port until the next server restart.
- LOGINSERVER_PORT is the port on which the Log in Service listens. If you specify **0**, the MWTM software uses a random available port, 1024 and above. The MWTM maintains the chosen port until the next server restart.
- WEB_PORT is the port on which the MWTM web server listens. You must specify a port number; **0** is not allowed. To change the WEB_PORT number, use the **mwtm webport** command (see mwtm webport, page B-93).

Note If any of these port numbers change, you must restart the MWTM server before the changes take effect.

Set these parameters in the MWTM *client's System.properties* file:

RMIREGISTRY_PORT = 44742

CLIENT_PORT = 0

where:

- RMIREGISTRY_PORT is the port on which the server-side RMI naming server listens. This port number must match the one specified for the RMIREGISTRY_PORT on the server side.
- CLIENT_PORT is the port on which the MWTM client listens for RMI callbacks (unsolicited notifications):
  - If you specify CLIENT_PORT = 0, the MWTM software uses any available port, 1024 and above.
  - If you specify CLIENT_PORT with a single value other than 0, such as CLIENT_PORT = 33459, the MWTM software uses that port, and you can run only one MWTM client process at a time.
  - If you specify CLIENT_PORT with a range of values other than 0, such as CLIENT_PORT = 33459-33479, the MWTM software can use any of the ports in the range, including the beginning and ending ports, and you can run more than one MWTM client process at a time.

Note If any of these port numbers change, you must restart the MWTM client before the changes take effect.

The MWTM client's *System.properties* file resides in the *properties* directory:

- In Solaris/Linux, if you installed the MWTM software in the default directory, */opt*, then the location of the file is */opt/CSCOsgmClient/properties/System.properties*.

- In Windows, if you installed the MWTM software in the default directory, *C:\Program Files*, then the location of the file is *C:\Program Files\SGMClient\properties\System.properties*.
- If you installed the MWTM software in a different directory, then the file resides in that directory.

Configuring Firewalls

Step 1 Identify the TCP port numbers to use between the MWTM server and client applications.

The MWTM software uses four TCP port numbers on the server side and two TCP port numbers on the client side to communicate between the MWTM server and client(s). These ports include the RMI Registry Port, the Data Server Port, the Login Server Port, the Client Port, and the HTTP Web Server port.

These ports are used for two way TCP connections between the MWTM server and client as follows:

1. For a client initiating a connection to the server, the initiating port on the client side is dynamic, and the target port on the server can be fixed by the DATASERVER_PORT and LOGINSERVER_PORT properties on the server.
2. For the server initiating a connection to the client (this is used for status change notifications), the initiating port on the server side is dynamic, and the target port on the client can be fixed by the CLIENT_PORT property on the client side.

You configure these port numbers in a plain-text file named *System.properties* located on the MWTM server and client. When configuring the MWTM software in a firewall deployment, you should use these port numbers:

- **RMI Registry Port**—44742
- **Data Server Port**—44751
- **Login Server Port**—44752
- **Client Port**—56173
- **HTTP Web Server Port**—1774

Step 2 Modify the *System.properties* file on the MWTM server. The *System.properties* file resides on the MWTM server under the */opt/CSCOsgm/properties* directory.

Note If the you installed the MWTM software in a location other than the default (*/opt/CSCOsgm*), substitute the correct directory name to locate the properties directory.

Caution Before editing, always make a backup of the file. This ensures a valid file exists in case an error is made during the editing process.

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

Port Name	Keyword	Value
RMI Registry Port	RMIREGISTRY_PORT	44742
Data Server Port	DATASERVER_PORT	44751

Port Name	Keyword	Value
Login Server Port	LOGINSERVER_PORT	44752
HTTP Web Server Port	WEB_PORT	1774

Step 3 Modify the *System.properties* file on the MWTM client. The *System.properties* file resides on the MWTM client machine under:

- /opt/CSCOsgm/properties directory for Solaris clients
- *C:\Program Files\MWTMClient\properties* for Windows clients

Note If the you installed the MWTM software in a location other than the default (*/opt/CSCOsgmClient*), substitute the correct directory name to locate the properties directory.

Caution Before editing, always make a backup of the file. This ensures a valid file exists in case an error is made during the editing process.

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

Port Name	Keyword	Value
RMI Registry Port	RMIREGISTRY_PORT	44742
Client Port	CLIENT_PORT	56173

Step 4 Modify the node configuration files with the chosen 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 the MWTM client and server, you can use the following extended access list:

Note The *established* entries are necessary, as they allow data to flow between the server and client that initiated the session. Without this keyword, clients will not have access to the MWTM server.

```
# MWTM Client Interface
interface FastEthernet 1/1
  ip address 192.168.1.100 255.255.255.0
  ip access-group client-to-server in

# MWTM Server Interface
interface FastEthernet 2/1
  ip address 192.168.2.100 255.255.255.0
  ip access-group server-to-client in

# Access list from client to server
ip access-list extended client-to-server
  10 permit tcp any any established
  20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44742
  30 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44751
  40 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44752
  50 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 1774
```

```
# Access list from server to client
ip access list extended server-to-client
  10 permit tcp any established
  20 permit tcp host 192.168.2.2 192.168.1.0 0.0.0.255 eq 56173
```

Step 5 Restart the MWTM server to use the newly chosen TCP port numbers.

As the root user, on the MWTM server, type:

```
#/opt/CSCOsgm/bin
#./mwtm restart
```

The server processes restart using the newly chosen port numbers.

Sample Firewall Configuration

This sample shows how to configure your firewall from the server side, client side, and Cisco node side.

Figure H-5 shows a sample firewall network with these parameters set in the *System.properties* file:

- On the MWTM server side:

  RMIREGISTRY_PORT = 44742

  DATASERVER_PORT = 44751

  LOGINSERVER_PORT = 44752

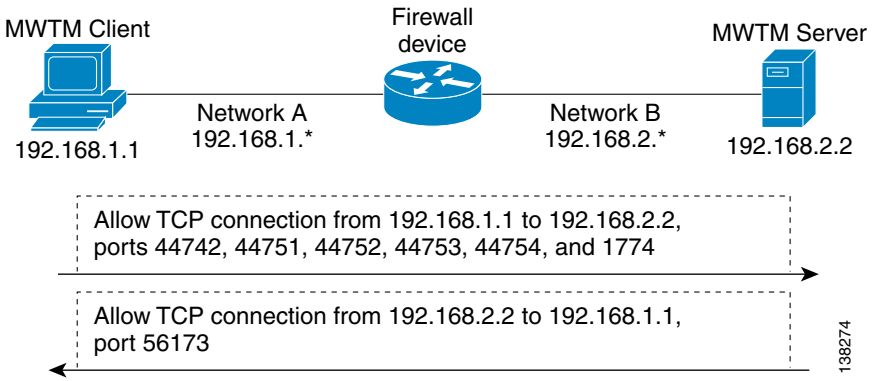
  WEB_PORT = 1774

- On the MWTM client side:

  RMIREGISTRY_PORT = 44742

  CLIENT_PORT = 56173

Figure H-5 Firewall Communication



This example illustrates a typical firewall configuration for Cisco nodes using access lists. This examples has two extended access lists:

- **ip access-list extended client-to-server**—This access list is applied on the input interface from the client to the server (FE 1/1).
- **ip access-list extended server-to-client**—This access list is applied on the input interface from the server to the client (FE 2/1).

```
!
ip access-list extended client-to-server
    10 permit tcp any any established
    20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44742
    30 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44751
    40 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44752
    50 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 1774
!   60 …
!
ip access list extended server-to-client
    10 permit tcp any any established
    20 permit tcp host 192.168.2.2 192.168.1.0 0.0.0.255 eq 56173
!   30 …
!
interface FastEthernet 1/1
    ip address 192.168.1.100 255.255.255.0
    ip access-group client-to-server in
!   …
!
interface FastEthernet 2/1
    ip address 192.168.2.100 255.255.255.0
    ip access-group server-to-client in
!   …
!
```

Note Both of these access lists allow established TCP connections (*10 permit tcp any any established, see previous*). When the MWTM 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.

Port-Forwarding Communication

To enable the MWTM software to operate in a TCP port-forwarding environment, perform these configuration tasks:

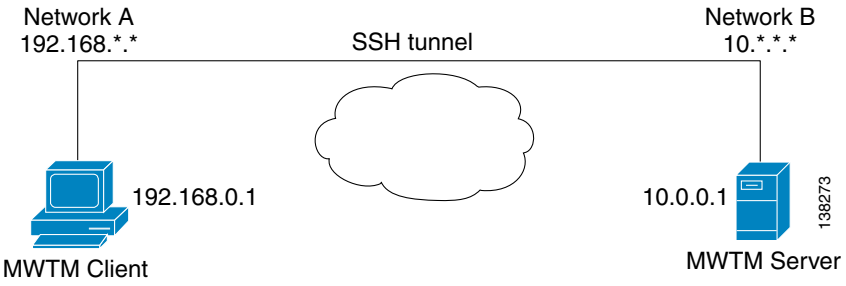
Step 1 Configure the server hostname and port number mapping in the MWTM client's *RMIOverNAT.properties* file, as described in NAT Communication, page H-4.

Step 2 Configure the port numbers used by the MWTM client and server in the *System.properties* file, as described in Firewall Communication, page H-5.

Step 3 Configure the port-forwarding tunnel to forward each side's TCP connection to the other side.

Figure H-6 shows a sample network that uses Secure Shell (SSH) port-forwarding. Other port-forwarding configurations might use a single host with dual interfaces at the client's and server's networks. While other port-forwarding configurations might differ from this example, the general rules to configure the MWTM software to operate in a port-forwarding environment are the same.

Figure H-6 Port-Forwarding Communication



The port-forwarding network shown in Figure H-6 has these parameters set:

- In the *System.properties* file, on the MWTM server side:

  RMIREGISTRY_PORT = 44742

  DATASERVER_PORT = 44751

  LOGINSERVER_PORT = 44752

  WEB_PORT = 1774

- In the *System.properties* file, on the MWTM client side:

  RMIREGISTRY_PORT = 44742

  CLIENT_PORT = 56173

- In the MWTM client's *RMIOverNAT.properties* file:

  10.0.0.1/44742 = 127.0.0.1/25742

  10.0.0.1/44751 = 127.0.0.1/25751

  10.0.0.1/44752 = 127.0.0.1/25752

  10.0.0.1/1774 = 127.0.0.1/8080

- In the port-forwarding network:

  Local port 25751 => remote host 127.0.0.1, port 44742

  Local port 25751 => remote host 127.0.0.1, port 44751

  Local port 25752 => remote host 127.0.0.1, port 44752

  Local port 8080 => remote host 127.0.0.1, port 1774

  Remote port 56173 => local host 127.0.0.1, port 56173

Note For port-forwarding setup, the backward-forwarding port numbers must match each other. In the previous example, both are 56173. The forward-forwarding port numbers do not need to match each other.

If you want to run more than one MWTM client process at the same time on the same node, you must specify CLIENT_PORT with a range of values other than 0, such as CLIENT_PORT = 33459-33479, in the MWTM client's *RMIOverNAT.properties* file. See Firewall Communication, page H-5 for more information about specifying the CLIENT_PORT parameter. You must also set up the backward-forwarding port numbers to use a range of values.

When the MWTM server starts, underlying network services register with the RMI server and publish themselves with the IP address specified in the SERVER_NAME property of the *System.properties* file on the MWTM server. In the given example, the published IP address is 10.0.0.1.

The MWTM client starts and connects to the localhost/127.0.0.1 (specified as the MWTM client's default server address). The SSH port-forwarding tunnel forwards the MWTM client's request to the RMI server at the MWTM server's localhost/127.0.0.1.

The MWTM client then asks where the MWTM services are located, and the RMI server replies that these MWTM services reside at 10.0.0.1. Without the *RMIOverNAT.properties* file on the MWTM client, the client would try to connect to 10.0.0.1, which would fail because of a network routing problem.

If we have configured the *RMIOverNAT.properties* file on the MWTM client as in the example, the MWTM client will still connect to the localhost/127.0.0.1 for name lookup, and the name server would return that MWTM services are running on 10.0.0.1. The MWTM client then looks in the *RMIOverNAT.properties* file, and discovers that the translated address for 10.0.0.1 is 127.0.0.1. With this configuration, the MWTM client will try to connect to 127.0.0.01 for RMI services (instead of 10.0.0.1). As a result, the connection will establish successfully.

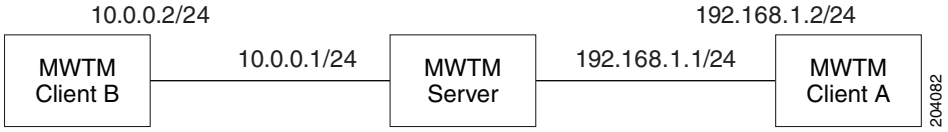
Configuring MWTM to Work With a Dual-Interface Machine Connected to Separate Networks

The MWTM client and server communication is based on Java RMI protocol. A limitation of RMI is its inability to publish itself with more than one specific IP address. This means that the RMI service can only register to one single interface on a dual interface machine. You can deploy the MWTM server on a dual interface machine in various scenarios:

- In some scenarios, all MWTM clients run on one side of the MWTM server interface, with no MWTM clients on the other side of the interface (for example, the other MWTM server interface is exclusively used for network management/SNMP traffic). In this scenario, ensure that the MWTM server published address is the interface connected to the MWTM clients. To change the published address of the MWTM server, see mwtm servername, page B-62.
- In some other scenarios, the two MWTM server interfaces are connected to the same network, or the two interfaces are connected to two different networks, but these networks are routed between each other. Typically, the intention is to use two physical interfaces to provide redundancy on the MWTM server. When providing physical interface redundancy, you should use Cisco Server Load Balancing technology. For details on configuring the MWTM software with this scenario, see Configuring MWTM with IOS Server Load Balancing, page H-16.

This section describes a third scenario: how to configure the MWTM software to work with a dual-interface machine that is connected to two separate networks. Both networks have MWTM clients that need to connect to the MWTM server. Figure H-7 is a diagram of a sample network where a single MWTM server is connected to two separate networks. Two MWTM clients, A and B, are on these two separate networks and need to communicate with the MWTM server.

Figure H-7 Sample Network



In this network configuration, the two networks (192.168.1.0/24 and 10.0.0.0/24) are not routed between each other. If the two networks were routed between each other (for example, if MWTM client B at 10.0.0.2 could reach the MWTM server at 192.168.1.1), you would configure the MWTM server with the 192.168.1.1 address, which would enable MWTM client A and MWTM client B to connect to the MWTM server.

The following sections give an example of how to configure the MWTM software to work with MWTM clients on both networks.

MWTM Server Configuration

The MWTM server can publish only one single IP address on the MWTM server machine. To configure this published address, use the **mwtm servername** command (see mwtm servername, page B-62).

For example, a system administrator configures the MWTM server to use the 192.168.1.1 address, by running the command **mwtm servername 192.168.1.1** on the MWTM server machine. The MWTM server will restart for the change to take effect. The command changes the *System.properties* file on the MWTM server to contain following line:

```
SERVER_NAME = 192.168.1.1
```

MWTM Client A Configuration

No special configurations are required on MWTM client A. Because this client is on the same network as the MWTM server binding interface, MWTM client A can communicate freely with the MWTM server.

You do need to ensure that during installation, MWTM client A has set up the MWTM server IP address as 192.168.1.1.

If the initial installation has incorrect information, you can change the MWTM server IP address to 192.168.1.1 using the **mwtm servername** command, or you can use the Change Default MWTM Server option on the MWTM client menu. For detailed information, see mwtm servername, page B-62, or Changing the Default MWTM Server Name, page 3-26.

MWTM Client B Configuration

When the MWTM server starts up on a dual-interface machine, it starts the RMI server and binds it to all the interfaces.

The MWTM server then starts all MWTM services and binds them to all the interfaces. These MWTM services then register with the RMI server and publish themselves with the IP address specified in the SERVER_NAME property of the *System.properties* file on the MWTM server. In the given example, the published IP address is 192.168.1.1.

MWTM client B starts up, connecting to 10.0.0.1 (specified as the MWTM client B default server address). MWTM client B connects to the RMI server at 10.0.0.1.

MWTM client B then asks where the MWTM services are located. The RMI server replies that these MWTM services reside at 192.168.1.1. Without the *RMIOverNAT.properties* file on the MWTM client B, the client would try to connect to 192.168.1.1, which would fail.

If we have configured the *RMIOverNAT.properties* file on MWTM client B as in the example, MWTM client B will still connect to 10.0.0.1 for name lookup, and the name server will return that MWTM services are running on 192.168.1.1. The MWTM client then looks in the *RMIOverNAT.properties* file, and discovers that the translated address for 192.168.1.1 is 10.0.0.1. With this configuration, MWTM client B will try to connect to 10.0.0.1 (instead of 192.168.1.1) for RMI services. As the result, the connection will establish successfully.

Configuring MWTM client B involves two things:

- First, ensure that MWTM client B has setup the MWTM server IP address as 10.0.0.1 during installation.

  If the initial installation has incorrect information, you can also change the MWTM server IP address to 10.0.0.1 using the **mwtm servername 10.0.0.1** command, or using the Change Default MWTM Server option on the MWTM client menu.

- Next, you must edit the *RMIOverNAT.properties* file on the MWTM client machine. On a Windows client, the default location of this file is *C:\ProgramFiles\SGMClient\properties\RMIOverNAT.properties*. On a Solaris client, the default location of this file is */opt/CSCOmwcClient/properties/RMIOverNAT.properties*.

  Add this line in the *RMIOverNAT.properties* file:

  ```
  192.168.1.1 = 10.0.0.1
  ```

After you have completed these steps, MWTM client B will be able to connect to the MWTM server even if the MWTM server published address 192.168.1.1 is unreachable from MWTM client B. MWTM client B will convert 192.168.1.1 to a reachable IP address 10.0.0.1 for client to server TCP connection.

Additional Network Configurations

Numerous other network configurations are not directly addressed here. The MWTM client and server can work with most of these networks, as long as the MWTM client and server can establish an SSH connection.

A few examples of alternative network configurations are:

- Dynamic NAT, where the MWTM client and server are on two different sides of the dynamic NAT network.
- A situation where the MWTM client is in a trusted network and the MWTM server is in a public network, but the firewall does not allow a direct TCP connection made from the MWTM server to the MWTM client.
- A situation where the MWTM server is in a trusted network and the MWTM client is in a public network, but the firewall does not allow a direct TCP connection made from MWTM client to MWTM server.

To allow the MWTM client and server communication in these network environments, you can establish a SSH connection between the MWTM client and the MWTM server using SSH port-forwarding (for details, see Port-Forwarding Communication, page H-10).

SSL Communication

If SSL is implemented and enabled in your MWTM system, the MWTM software uses secure socket communication for both RMI and HTTP communication between the MWTM client and server.

The MWTM software supports standard-based SSL encryption algorithms, including RSA, DSA public key algorithms, and 40-bit or 128-bit encryption. The MWTM software can generate an X.509 certificate and a certificate signing request (CSR), which is interoperable with most certificate authorities (CAs).

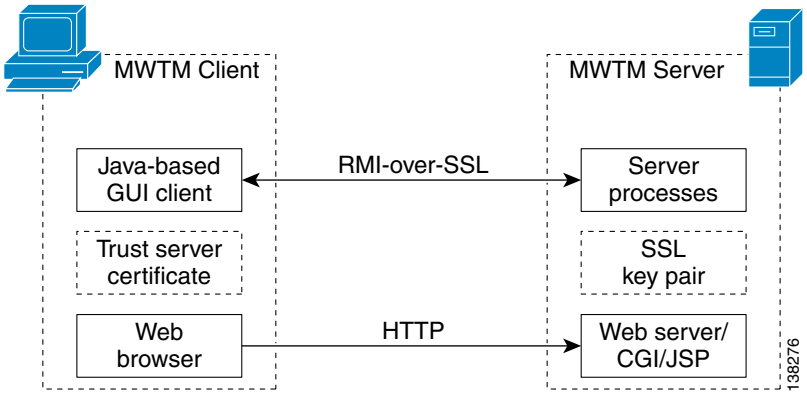
Both the MWTM web server and the MWTM server processes share the same SSL key/certificate pair. In addition, the MWTM client and the web browser can examine the server's certificate.

For more information, including descriptions of the MWTM commands and procedures used to implement, enable, manage, and monitor SSL support, see Implementing SSL Support in the MWTM, page 2-20.

Figure H-8 shows a sample MWTM-over-SSL network with these characteristics:

- A user-generated SSL key pair on the MWTM server.
- The server's certificate is trusted on the MWTM client.
- Communication between the client and server is RMI-over-SSL and HTTPS. Both protocols are encrypted and secure.

Figure H-8 SSL Communication



Configuring MWTM with IOS Server Load Balancing

If a network failure causes the MWTM software to fail, you can no longer monitor your network. You can solve this potential problem by configuring a backup MWTM server, as detailed in Configuring a Backup MWTM Server, page 3-10. However, this solution requires a connection to the backup MWTM server, which might not mirror exactly the primary MWTM server.

A better solution is to use IOS Server Load Balancing (IOS SLB), which provides transparent failover of the MWTM client connection.

Use this procedure to configure the MWTM software with IOS SLB:

Step 1 Ensure that you have this required hardware and software:

- Solaris/Linux server with at least two network interface cards (NICs)
- Cisco 7204VXR or 7206VXR series node
- IOS SLB release 12.1(11b)E or later
- MWTM release 6.1 or later

Step 2 Configure the Solaris/Linux server with at least two active NICs.

Step 3 Configure a routing protocol on the Solaris/Linux server, such that if one network interface fails, the other interfaces can still contact the monitored networks and the MWTM client:

- Run **in.routed** on the Solaris/Linux server, with two RIP-based nodes on two separate networks providing routing tables for the server. See the **in.routed** man page for more information on this configuration.
- Use the GateD routing software developed by NextHop Technologies.

Step 4 Configure the Cisco 7204VXR or 7206VXR series router, with the Solaris/Linux server network interfaces configured as real servers in the server farm. Refer to the IOS SLB feature module for more information on configuring the IOS SLB node.

Step 5 Configure a virtual interface, lo0:1 with the Internet address that matches the virtual IP address configured on the IOS SLB node:

ifconfig lo0:1 addif *ip-address*

Step 6 Install the MWTM software.

Step 7 Edit the */opt/CSCOsgm/properties/System.properties* file, and replace the SERVER NAME variable with the DNS entry that matches the virtual IP address configured on the IOS SLB node. Save your changes and restart the MWTM server.

Step 8 Configure your MWTM clients to match the same DNS entry.

Your configuration is complete.

Remember that:

- Failover of the MWTM client is transparent to the user. No additional changes are needed at that end.
- A failure of either interface, or of the surrounding networks, might cause the MWTM client to hang for a short period, depending on the convergence of the routing protocol used by the MWTM server. For example, with RIP, the MWTM client might hang for up to two minutes while RIP converges after a network failure. Faster protocols might result in shorter MWTM client hang times.