APPENDIX F

Configuring MWTM to Run with Various Networking Options

In addition to running on standard IP-connected networks, 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). MWTM 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. As shown in , this includes:

- Two-way 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 node'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.

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

This appendix includes the following sections:

- VPN Communication, page F-1
- NAT Communication, page F-2
- Firewall Communication, page F-3
- Port-Forwarding Communication, page F-7
- Additional Network Configurations, page F-9
- SSL Communication, page F-9

VPN Communication

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 needs to register with the MWTM server server using the correct IP address, so that the server can invoke RMI callbacks and send unsolicited notifications to the client.

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

shows a sample VPN network with the following 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.

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. This configuration is transparent to the user; no manual configuration is needed.

NAT Communication

MWTM client/server communication can run through one or more static NAT-connected networks. (MWTM does not support dynamic NAT or dynamic NAT pool overloading.)

In a static NAT network, the MWTM client and server are located 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 RMI protocol, this is not sufficient. 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 within the packet content. Therefore, the NAT device cannot recognize the IP address inside the packet, and fails to route it correctly.

MWTM solves this problem by creating a specialized NAT-aware socket factory. Some manual configuration on the part of the user is required to enable MWTM to “know” the network NAT configuration.

shows a sample static NAT network with the following 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 MWTM client IP address 192.168.0.1 in Network A to 10.1.1.2 in Network B.
- The NAT device maps MWTM server IP address 10.0.0.1 in Network B to 192.168.1.2 in Network A.

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

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

For the example shown in , you must add the following 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.

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.

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

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

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

Set the following parameters on the server side of the file:

RMIREGISTRY_PORT = 44742

DATASERVER_PORT = 0

MLSERVER_PORT = 0

PMSERVER_PORT = 0

LOGINSERVER_PORT = 0

WEB_PORT = 1744

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 sgmDataServer process listens. If you specify **0**, MWTM uses any available port, 1024 and above.
- **MLSERVER_PORT** is the port on which the sgmMsgLogServer process listens. If you specify **0**, MWTM uses any available port, 1024 and above.
- **PMSERVER_PORT** is the port on which the sgmProcMgrServer process listens. If you specify **0**, MWTM uses any available port, 1024 and above.
- **LOGINSERVER_PORT** is the port on which the Login service in the sgmDataServer process listens. If you specify **0**, MWTM uses any available port, 1024 and above.
- **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 the "mwtm webport" section on page C-75 for more information.

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

Set the following parameters in the MWTM client's *RMIOverNAT.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**, MWTM uses any available port, 1024 and above.
  - If you specify **CLIENT_PORT** with a single value other than **0**, such as **CLIENT_PORT = 33459**, MWTM 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**, MWTM 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.

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

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

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

shows a sample firewall network with the following parameters set in the *System.properties* file:

- On the MWTM server side:

  RMIREGISTRY_PORT = 44742

  DATASERVER_PORT = 44751

  MLSERVER_PORT = 44752

  PMSERVER_PORT = 44753

  LOGINSERVER_PORT = 44754

  WEB_PORT = 1774

- On the MWTM client side:

  RMIREGISTRY_PORT = 44742

  CLIENT_PORT = 56173

Port-Forwarding Communication

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

Step 1 Configure the server hostname and port number mapping in the MWTM client's *RMIOverNAT.properties* file, as described in the "NAT Communication" section on page F-2.

Step 2 Configure the port numbers used by the MWTM client and server in the *System.properties* file, as described in the "Firewall Communication" section on page F-3.

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

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 may differ from this example, the general rules to configure MWTM to operate in a port-forwarding environment are the same.

The port-forwarding network shown in has the following parameters set;

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

  RMIREGISTRY_PORT = 44742

  DATASERVER_PORT = 44751

  MLSERVER_PORT = 44752

  PMSERVER_PORT = 44753

  LOGINSERVER_PORT = 44754

  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

  10.0.0.1/44753 = 127.0.0.1/25753

  10.0.0.1/44754 = 127.0.0.1/25754

  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 25753 => remote host 127.0.0.1, port 44753

  Local port 25754 => remote host 127.0.0.1, port 44754

  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 above 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 device, 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 the "Firewall Communication" section on page F-3 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.

Additional Network Configurations

There are numerous other network configurations that 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 as follows:

- 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 wher e 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 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 F-7).

SSL Communication

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

MWTM supports standard-based SSL encryption algorithms, including RSA, DSA public key algorithms, and 40-bit or 128-bit encryption. MWTM 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. Both 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 the "Implementing SSL Support in MWTM (Solaris Only)" section on page 10-22.

shows a sample MWTM-over-SSL network with the following 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.