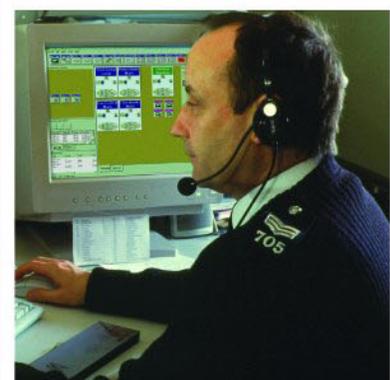


# MIP 5000 VoIP Radio Console VPN Solution Guide



2215247G-01  
OCTOBER 2010





# CONTENTS

.....

## ABOUT THIS BOOKLET

Intended Audience .....	ix
Assumptions .....	ix
References .....	x
Related Information .....	x

## CHAPTER 1: VPN SOLUTION

Throughput Requirements .....	1-2
Recommendations .....	1-3
Prerequisites .....	1-4
Dispatch Center Setup .....	1-5
Server-Side UT-3302 Installation .....	1-6
Server-Side UT-3302 Configuration .....	1-7
Remote Console Setup .....	1-10
Remote Console Preparation .....	1-11
Client-Side UT-3302 Configuration .....	1-13
Client-Side UT-3302 Installation .....	1-15
Remote Console Network Configuration .....	1-15

## GLOSSARY

## INDEX

**THIS PAGE INTENTIONALLY LEFT BLANK.**

# LIST OF FIGURES



Figure 1-1: Example MIP 5000 VPN Connection .....	1-3
Figure 1-2: Example MIP 5000 VPN Connection .....	1-5
Figure 1-3: Example MIP 5000 VPN Connection .....	1-10

**THIS PAGE INTENTIONALLY LEFT BLANK.**

# **LIST OF TABLES**



Table 1-1: MIP 5000 Throughput Requirements (Half Duplex).....1-2  
Table 1-2: MIP 5000 Throughput Requirements (Full Duplex) .....1-2

**THIS PAGE INTENTIONALLY LEFT BLANK.**

# **LIST OF PROCEDURES & PROCESSES**



Procedure 1-1: How to Install the Server-Side UT-3302 Bridge.....	1-6
Procedure 1-2: How to Configure the Server-Side UT-3302 Bridge .....	1-7
Procedure 1-3: How to Prepare for Client-Side Configuration .....	1-11
Procedure 1-4: How to Configure the Client-Side UT-3302 Bridge.....	1-13
Procedure 1-5: How to Install the Client-Side UT-3302 Bridge.....	1-15
Procedure 1-6: How to Configure the Client-Side Network .....	1-15

**THIS PAGE INTENTIONALLY LEFT BLANK.**

## **ABOUT THIS BOOKLET**

---

This booklet describes a virtual private network (VPN) solution that has been tested with MIP 5000 VoIP Radio Console. The VPN solution uses a pair of encrypted Ethernet bridges to provide a secure Ethernet tunnel between the dispatch center and a remote MIP 5000 console.

The secure Ethernet tunnel supports a remote console operator receiving audio from and transmitting audio to radio channels and other MIP 5000 consoles using AES encryption.

Testing was conducted using a pair of Data Comm for Business, Inc. UT-3302 bridges. This model supports the maximum throughput required for a remote MIP 5000 console to communicate with 24 half-duplex radio channels and 76 other MIP 5000 consoles or 24 full-duplex radio channels and 26 other MIP 5000 consoles. Other models of Ethernet tunnel bridge are available from Data Comm for Business that support higher throughput rates.

This document describes the installation and configuration activities required to support a secure Ethernet tunnel for MIP 5000 using a UT-3302 Encrypted Ethernet Tunnel.

## **INTENDED AUDIENCE**

---

This booklet has been written for readers who have a thorough understanding of networking principles and the IP protocol.

## **ASSUMPTIONS**

---

This guide makes the following assumptions:

- The VPN will provide a secure tunnel through the Internet.
- Static IP addressing is used for the MIP 5000 gateways and consoles.

## REFERENCES

- *UT-3302 Encrypted Ethernet Tunnel* data sheet (available at <http://www.dcbnet.com/datasheet/ut3302ds.html>)
- *UT-3302 Encrypted Ethernet Tunnel User's Guide* (available on the CD accompanying the UT-3302 bridge or at <http://www.dcbnet.com/manuals/ut3302manual.pdf>)

## RELATED INFORMATION

Refer to the following documents for associated information about the MIP 5000 system:

Related Manuals	Purpose
<i>MIP 5000 VoIP Radio Console System Planner</i>	Provides information necessary to plan a MIP 5000 VoIP Radio Console system
<i>MIP 5000 VoIP Radio Console Operator Manual</i> (6881013Y34)	Describes how to use a MIP 5000 VoIP Radio Console position
<i>MIP 5000 VoIP Radio Console Supervisor Manual</i> (6881013Y33)	Describes how to configure and customize MIP 5000 VoIP Radio Console positions
<i>MIP 5000 VoIP Radio Console Installation and Configuration Manual</i> (6881013Y35)	Describes how to install and configure a MIP 5000 system
<i>Motorola R56—Standards and Guidelines for Communication Sites</i> (6881089E50); also available on CD-ROM (9882904Y01)	Describes the standards and guidelines recommended for radio communication sites

## NOTICE

Motorola does not sell or support the VPN equipment described in this booklet. This booklet is intended only to aid users in establishing a VPN connection to a MIP 5000 network by describing one available solution. Motorola is not responsible for the performance of this VPN solution or for any changes made by Data Comm for Business, Inc. in the specifications or installation requirements of its Ethernet bridges.

# VPN SOLUTION

---

This chapter contains the following sections:

- “Throughput Requirements” on page 1-2
- “Recommendations” on page 1-3
- “Prerequisites” on page 1-4
- “Dispatch Center Setup” on page 1-5
  - “Server-Side UT-3302 Installation” on page 1-6
  - “Server-Side UT-3302 Configuration” on page 1-7
- “Remote Console Setup” on page 1-10
  - “Remote Console Preparation” on page 1-11
  - “Client-Side UT-3302 Configuration” on page 1-13
  - “Client-Side UT-3302 Installation” on page 1-15
  - “Remote Console Network Configuration” on page 1-15

## THROUGHPUT REQUIREMENTS

A UT-3302 Encrypted Ethernet Tunnel provides a data throughput rate of 10 Mbps. Communication with a single MIP 5000 gateway (channel) or console requires up to approximately 100 kbps of throughput in half-duplex mode and 200 kbps in full-duplex mode.

MIP 5000 throughput requirements for half-duplex systems of varying composition are listed in Table 1-1. Throughput requirements for full-duplex systems of varying compositions are listed in Table 1-2.

The UT-3302 bridges that were tested support a sustained throughput rate of 10 Mbps with encryption. Other models from the same manufacturer provide greater throughput rates, like the ET-6630, which provides a throughput rate of 200 Mbps.

**TABLE 1-1** MIP 5000 THROUGHPUT REQUIREMENTS (HALF DUPLEX)

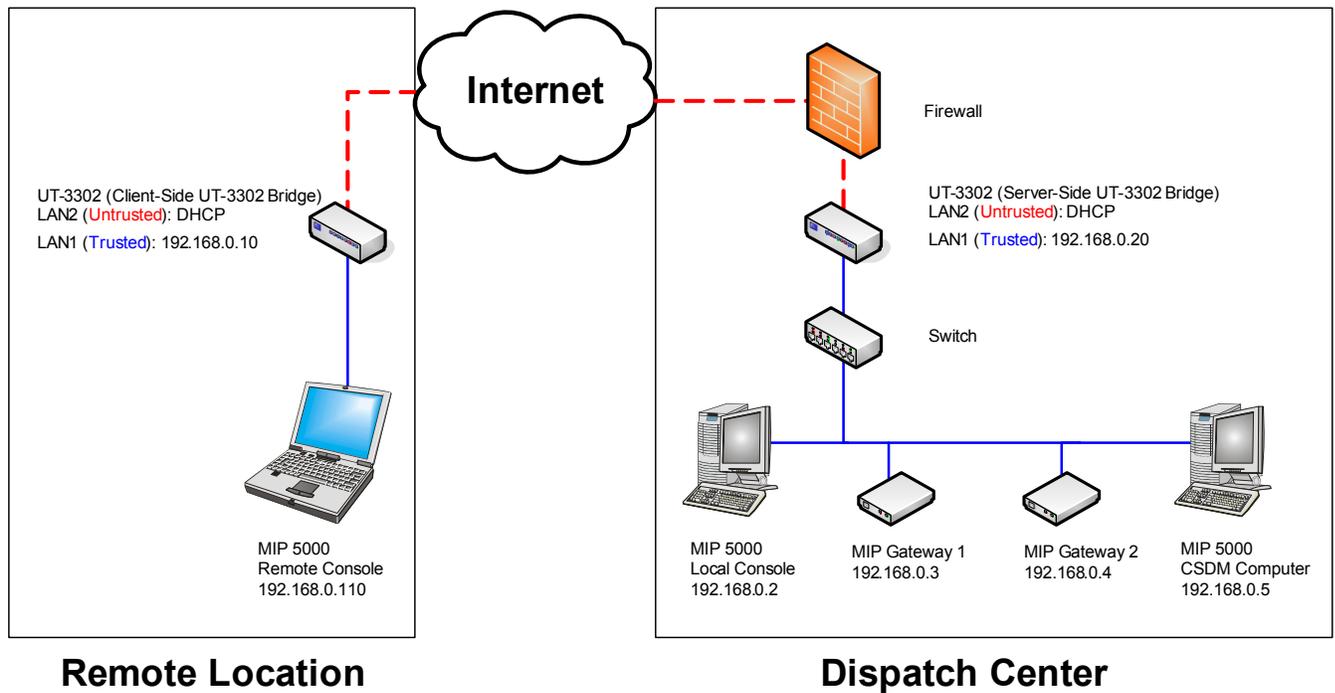
Remote Console Requirement	Maximum Throughput
1 channel, no other consoles	100 kbps
1 channel, 20 other consoles	2.1 Mbps
1 channel, 40 other consoles	4.1 Mbps
1 channel, 99 other consoles	10.0 Mbps
24 channels, no other consoles	2.4 Mbps
24 channels, 76 other consoles	10.0 Mbps
24 channels, 99 other consoles	12.4 Mbps <sup>1</sup>

**TABLE 1-2** MIP 5000 THROUGHPUT REQUIREMENTS (FULL DUPLEX)

Remote Console Requirement	Maximum Throughput
1 channel, no other consoles	200 kbps
1 channel, 20 other consoles	4.2 Mbps
1 channel, 40 other consoles	8.2 Mbps
1 channel, 99 other consoles	20.0 Mbps <sup>1</sup>
24 channels, no other consoles	4.8 Mbps
24 channels, 26 other consoles	10.0 Mbps
15 channels, 35 other consoles	10.0 Mbps
24 channels, 99 other consoles	24.8 Mbps <sup>1</sup>

1. The configurations shown in shaded rows require greater throughput rates than the UT-3302 bridge provides.

FIGURE 1-1 EXAMPLE MIP 5000 VPN CONNECTION

**Legend**

**Untrusted** — Connections over the Internet

**Trusted** — Connections within your secure network

Server-Side UT-3302 Bridge — VPN bridge at Dispatch Center

Client-Side UT-3302 Bridge — VPN bridge at Remote Location

Remote Console — MIP 5000 console at Remote Location

## RECOMMENDATIONS

.....

.....

A pair of UT-3302 bridges supports the joining of two separate networks at two locations as parts of a single subnet. We recommend configuring your MIP 5000 network as though the dispatch center and the remote console were parts of a single subnet. This means that the trusted port of both UT-3302 bridges must use IP addresses within a single subnet range.

Because the default UT-3302 IP address of 192.168.0.1 may not be appropriate for your local network, we recommend connecting the DCB UT-3302 bridges for the first time using the serial cable to change their IP addresses (that is, the IP address on the trusted side) to the addresses that they will use when connected to your network.

After changing the IP address, then connect each bridge to the network and direct your Web browser to the bridge using a secure connection (https) to continue configuration. Be sure not to connect through a proxy server. The minimum configuration items required for basic LAN-to-LAN bridging connection may all be entered using the *Quick Setup* menu screen.

## PREREQUISITES

---

Certain prerequisites must be in place for both the dispatch center setup and the remote console setup.

The following dispatch center prerequisites are needed:

- IP address for the trusted connection of the server-side UT-3302 bridge
- Subnet mask for the trusted connection of the server-side UT-3302 bridge

The following remote console site prerequisites are needed:

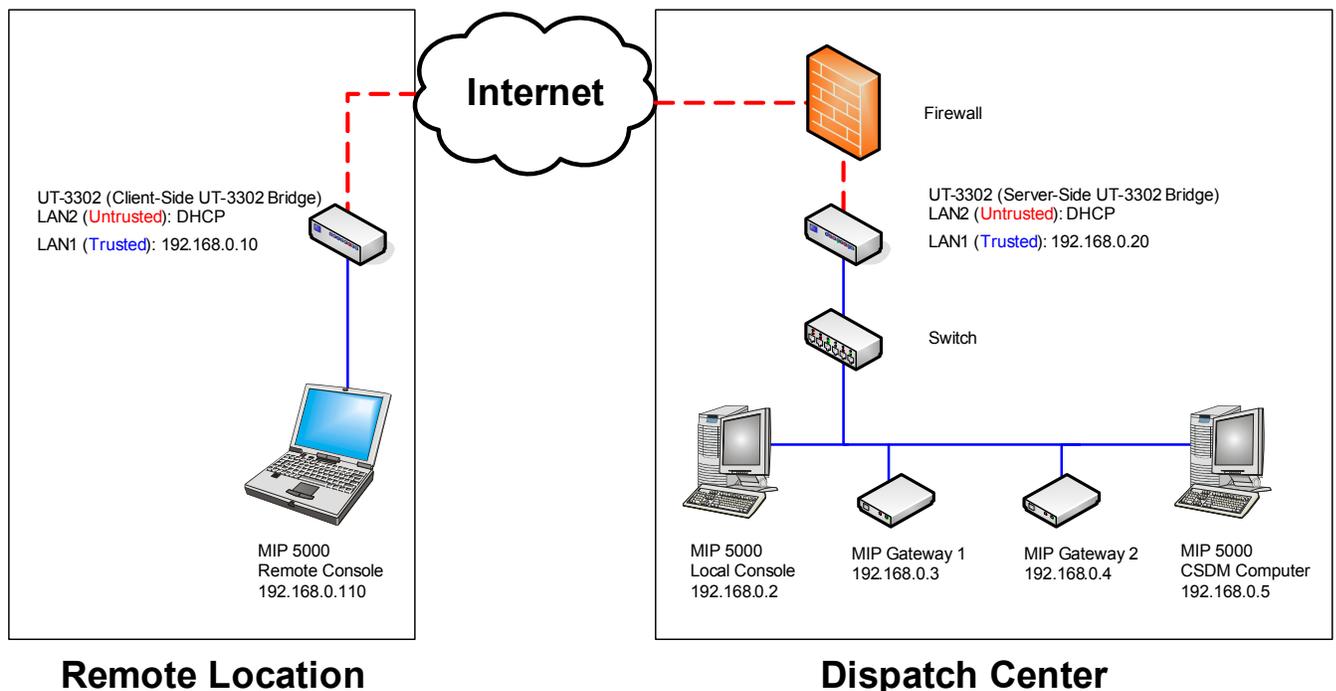
- IP address for the trusted connection of the client-side UT-3302 bridge, which must be a member of the same subnet as the server-side UT-3302 bridge
- IP address for the remote console computer, which must be a member of the same subnet as the two UT-3302 bridges
- Subnet mask for the trusted connection of the client-side network entities (console computer, bridge, router)
- IP address of the untrusted connection of the server-side UT-3302 bridge, assigned automatically by DHCP
- Fully installed and configured MIP 5000 VoIP Radio Console computer with all necessary peripheral equipment. Peripheral equipment can include some or all of these items:
  - Headset
  - Speakers
  - Microphone
  - Jackbox
- A wireline Ethernet interface with RJ45 connection to the Internet

# DISPATCH CENTER SETUP

The following activities are required to prepare the dispatch center for VPN connection:

- “Server-Side UT-3302 Installation” on page 1-6
- “Server-Side UT-3302 Configuration” on page 1-7

**FIGURE 1-2** EXAMPLE MIP 5000 VPN CONNECTION



**Legend**

Untrusted — Connections over the Internet

Trusted — Connections within your secure network

Server-Side UT-3302 Bridge — VPN bridge at Dispatch Center

Client-Side UT-3302 Bridge — VPN bridge at Remote Location

Remote Console — MIP 5000 console at Remote Location

## SERVER-SIDE UT-3302 INSTALLATION

Install the server side UT-3302 bridge.

### PROCEDURE 1-1 HOW TO INSTALL THE SERVER-SIDE UT-3302 BRIDGE

- 1 Identify an IP address to assign to LAN1 (trusted) of the server-side UT-3302 bridge.
- 2 Change the default IP address of the server-side UT-3302 to use the assigned IP address, as described in the *UT-3302 Encrypted Ethernet Tunnel User's Guide*.



#### EXAMPLE

In Figure 1-2, "Example MIP 5000 VPN Connection," the IP address used is 192.168.0.20.



#### NOTE

Setting the default IP address also sets the LAN1 IP address of the UT-3302 bridge.

- 3 Connect the Untrusted port of the UT-3302 bridge so that it is accessible from the Internet and reboot the bridge by powering it off and then on.



#### NOTE

The UT-3302 bridge should be installed on the trusted side of any firewall devices that are between the MIP 5000 network and the Internet.

If required by your network firewall, create an exception to allow the UT-3302 bridge to receive incoming data at its server port (22).

- 4 Connect one of the Trusted ports of the UT-3302 bridge to any Ethernet port on any switch connected to the dispatch center LAN.

**Result:** The UT-3302 bridge is inserted between the dispatch center LAN and the Internet.



#### NOTE

The dispatch center LAN is the network to which MIP 5000 VoIP Radio Consoles are connected.

## SERVER-SIDE UT-3302 CONFIGURATION

Configure the server-side UT-3302 bridge.

### PROCEDURE 1-2 HOW TO CONFIGURE THE SERVER-SIDE UT-3302 BRIDGE

- 
- 1 Make a secure connection (using https) to the UT-3302 bridge with a Web browser from anywhere in the network using the IP address configured in step 2 of Procedure 1-1.
  - 2 Log in as described in the *UT-3302 Encrypted Ethernet Tunnel User's Guide*.
  - 3 In the **MENU** pane, select **Quick Setup**.  
**Result:** The **Quick Setup** menu appears.
- 

- 4 On the **Quick Setup** menu, fill in or verify the **LAN1 (trusted)** fields as described below:
  - **LAN1 Configure IP** — Static-Configuration
  - **LAN1 IP Address** — <IP address of this bridge, as set at step 2 of Procedure 1-1.>
  - **LAN1 Subnet Mask** — <subnet mask appropriate for the subnet of which this bridge is a member>
  - **LAN1 Gateway** — (Leave empty)



#### NOTE

If the remote console computer needs access to any gateways or consoles that are located in another subnet in the dispatch center network, then put the IP address of the default gateway for the subnet in which the remote console computer is located in the **LAN1 Gateway** field.

- 
- 5 On the **Quick Setup** menu, fill in the **LAN2 (untrusted)** fields as described below:
    - **LAN2 Configure IP** — automatic-via-DHCP
    - **LAN2 IP Address** — (Leave empty)
    - **LAN2 Subnet Mask** — (Leave empty)
    - **LAN2 Gateway** — (Leave empty)
-

**PROCEDURE 1-2** HOW TO CONFIGURE THE SERVER-SIDE UT-3302 BRIDGE (CONTINUED)

- 
- 6** On the **Quick Setup** menu, fill in the **Ethernet Tunnel** fields as described below:
- **Shared Secret** — *<secret phrase that must be the same on client and server bridges, can be up to 52 characters, no quote or backslash>*
  - **Encryption** — 128 bit, 192 bit, or 256 bit AES  
*Encryption setting must be the same on client and server bridges.*
  - **Mode** — server
  - **Authorized Client Name1** — *<user name that must be the same as Client Name on client bridge, can be up to 52 characters, no quote or backslash>*
  - **Authorized Client Password1** — *<user password that must be the same as Client Password on client bridge, can be up to 52 characters, no quote or backslash>*
  - **Server Port** — *<server port used by server-side UT-3302 bridge; default is 22>*
  - **Client Name** — (Leave empty)
  - **Client Password** — (Leave empty)
  - **Remote Server IP** — (Leave empty)
  - **Remote Server Port** — (Leave empty)
  - **Interface** — (Leave empty)
- 

- 7** Click **Store & Activate**.

**Result:** The new settings are saved and made active. The DHCP server assigns the server-side bridge an IP address for LAN2 (untrusted).

**NOTE**

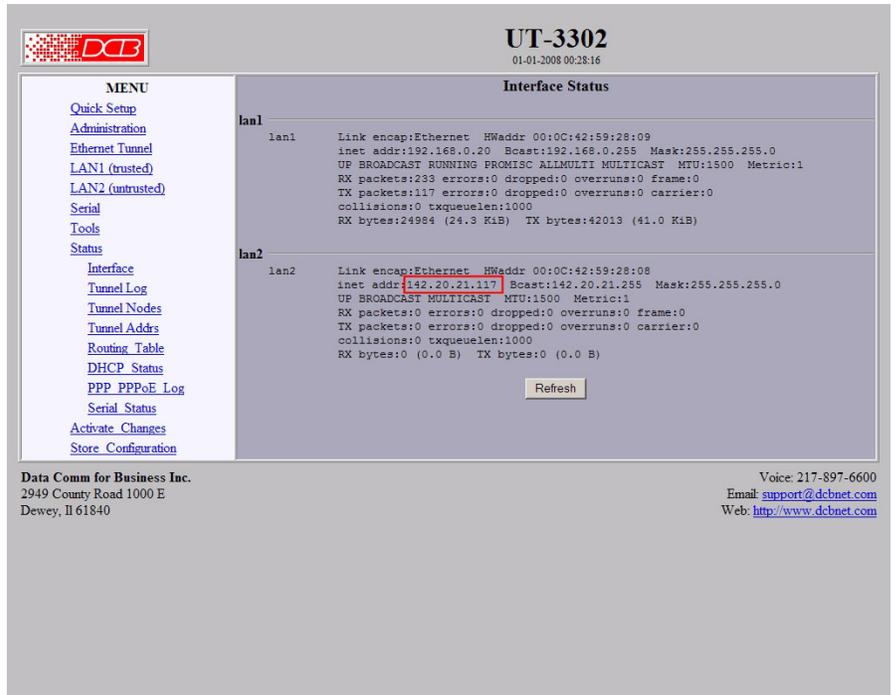
The IP address assigned by the DHCP server for LAN2 (untrusted) is needed for the configuration of the client-side bridge.

---

**PROCEDURE 1-2** HOW TO CONFIGURE THE SERVER-SIDE UT-3302 BRIDGE (CONTINUED)

- 8** In the MENU pane, select **Status**.

**Result:** The **Interface Status** report appears.



**UT-3302**  
01-01-2008 00:28:16

**Interface Status**

**lan1**

```
lan1  Link encap:Ethernet  HWaddr 00:0C:42:59:28:09
      inet addr:192.168.0.20  Bcast:192.168.0.255  Mask:255.255.255.0
      UP BROADCAST RUNNING PROMISC ALLMULTI MULTICAST  MTU:1500  Metric:1
      RX packets:233  errors:0  dropped:0  overruns:0  frame:0
      TX packets:117  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0  txqueuelen:1000
      RX bytes:24984 (24.3 KiB)  TX bytes:42013 (41.0 KiB)
```

**lan2**

```
lan2  Link encap:Ethernet  HWaddr 00:0C:42:59:28:08
      inet addr:142.20.21.117  Bcast:142.20.21.255  Mask:255.255.255.0
      UP BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0  errors:0  dropped:0  overruns:0  frame:0
      TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0  txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Refresh

**MENU**

- [Quick Setup](#)
- [Administration](#)
- [Ethernet Tunnel](#)
- [LAN1 \(trusted\)](#)
- [LAN2 \(untrusted\)](#)
- [Serial](#)
- [Tools](#)
- [Status](#)
- [Interface](#)
- [Tunnel Log](#)
- [Tunnel Nodes](#)
- [Tunnel Addr](#)
- [Routing Table](#)
- [DHCP Status](#)
- [PPP PPPoE Log](#)
- [Serial Status](#)
- [Activate Changes](#)
- [Store Configuration](#)

Data Comm for Business Inc.  
2949 County Road 1000 E  
Dewey, IL 61840

Voice: 217-897-6600  
Email: [support@dcnet.com](mailto:support@dcnet.com)  
Web: <http://www.dcnet.com>

- 9** Make note of the IP address identified as **lan2** — **inet addr**, highlighted by the red rectangle in the illustration above.

**Result:** The noted IP address is available for use when configuring the client-side UT-3302 bridge.

**NOTE**

You will need to enter this IP address at step 7 of Procedure 1-4.

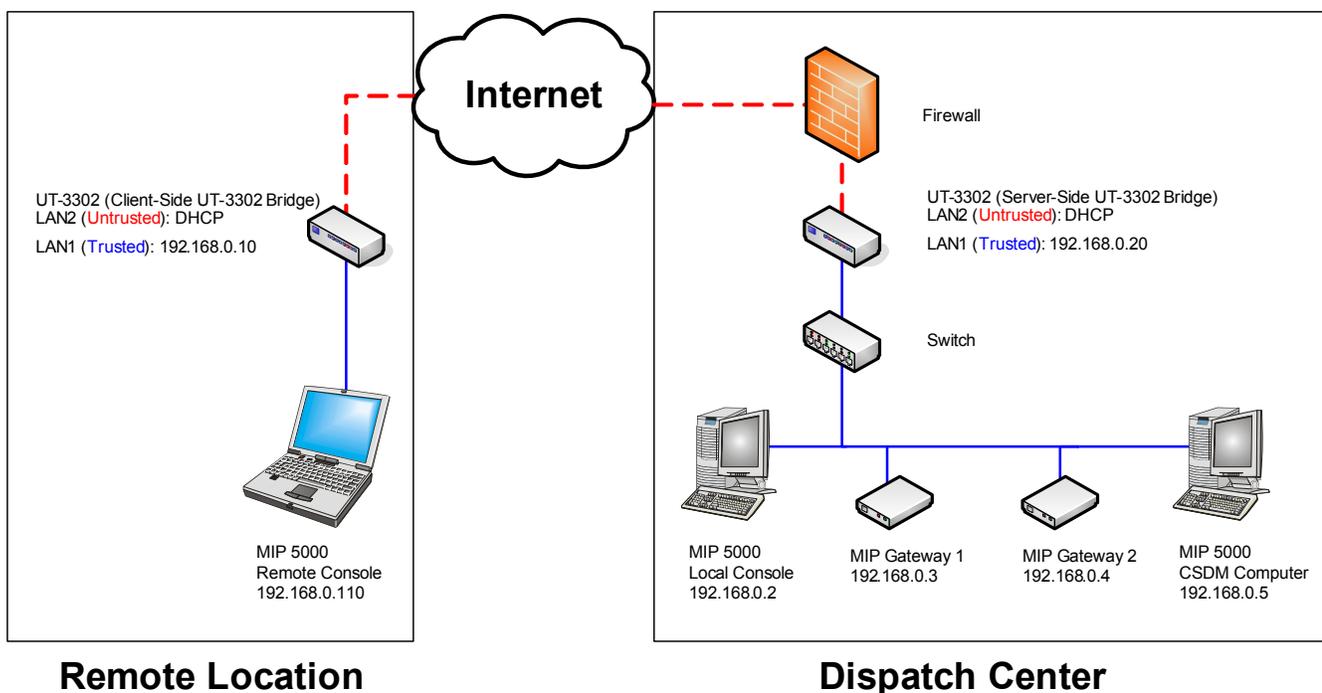
- 10** Close your browser.

# REMOTE CONSOLE SETUP

The following procedures are required to install and configure the remote MIP 5000 console:

- “Remote Console Preparation” on page 1-11
- “Client-Side UT-3302 Configuration” on page 1-13
- “Client-Side UT-3302 Installation” on page 1-15
- “Remote Console Network Configuration” on page 1-15

**FIGURE 1-3** EXAMPLE MIP 5000 VPN CONNECTION



**Legend**  
**Untrusted** — Connections over the Internet  
**Trusted** — Connections within your secure network  
 Server-Side UT-3302 Bridge — VPN bridge at Dispatch Center  
 Client-Side UT-3302 Bridge — VPN bridge at Remote Location  
 Remote Console — MIP 5000 console at Remote Location

## REMOTE CONSOLE PREPARATION

Certain preparatory activities must be carried out at the dispatch center before the remote VPN MIP 5000 console is deployed. For example, the console computer must have the MIP 5000 VoIP Radio Console software installed, IP addresses must be assigned for the console and the remote bridge, and the configuration database must be updated with the IP address that the remote console will be using.

### PROCEDURE 1-3 HOW TO PREPARE FOR CLIENT-SIDE CONFIGURATION

---

**1** Identify IP addresses to assign to these client-side network entities:

- UT-3302 bridge, LAN1 (trusted)
- MIP 5000 VoIP Radio Console computer

The IP address of the console computer must be registered in the CSDM as the **DCPM IP Address**.



#### NOTE

These addresses are needed for this procedure (Procedure 1-3), Procedure 1-4, and Procedure 1-6.

---

**2** If you have not already done so, install the MIP 5000 VoIP Radio Console program on the remote console and, if possible, test it in the dispatch center using a local Ethernet connection.



#### SUGGESTION

By testing the remote console at the dispatch center, you can eliminate the console and its configuration as possible causes of failures in the field.

---

**3** Use the CSDM computer in the dispatch center to prepare the other parts of the system (gateways and other consoles) for the remote console, as described in steps 4, 5, and 6.



#### NOTE

The remote console does not need to be connected while you perform these activities.

---

**PROCEDURE 1-3 HOW TO PREPARE FOR CLIENT-SIDE CONFIGURATION (CONTINUED)**

- 4 Update the CSDM entry for the remote VPN console to use the IP address assigned in step 1 for **DCPM IP Address** and the physical (MAC) address of the remote console computer for **MAC Address**.

- 5 From the **Options** menu, select **Generate Configuration Files**, then click **Generate**.

**Result:** The MIP 5000 configuration database is made available to consoles and gateways.

- 6 At any active MIP 5000 console, use the configuration password to gain Allow Layout Reconfiguration access.

- 7 Select **Edit > Channels Configuration** and, for each channel that the remote VPN console will access, select the channel in the list of channels and click **Database Upload Radio Gateway**.

**Result:** The MIP 5000 gateway for each channel that the console will use is updated to recognize the console.

## CLIENT-SIDE UT-3302 CONFIGURATION

The client-side UT-3302 bridge does not need to be at the remote console location when you carry out Procedure 1-4. If you wish, this activity can take place in a lab or at the dispatch center.

### PROCEDURE 1-4 HOW TO CONFIGURE THE CLIENT-SIDE UT-3302 BRIDGE

- 1 Change the default IP address of the client-side UT-3302 to use the IP address assigned in step 1 of Procedure 1-3, as described in the *UT-3302 Encrypted Ethernet Tunnel User's Guide*.



#### EXAMPLE

In Figure 1-3, "Example MIP 5000 VPN Connection," the IP address used is 192.168.0.10.



#### NOTE

Setting the default IP address also sets the LAN1 IP address of the UT-3302 bridge.

- 2 Make a secure connection (using https) to the UT-3302 bridge with a Web browser from anywhere in the network using the IP address configured in step 1.
- 3 Log in as described in the *UT-3302 Encrypted Ethernet Tunnel User's Guide*.
- 4 Select the **Quick Setup** menu.
- 5 On the **Quick Setup** menu, fill in or verify the **LAN1 (trusted)** fields as described below:
  - **LAN1 Configure IP** — Static-Configuration
  - **LAN1 IP Address** — <IP address of this bridge, as set in step 1 of this procedure>
  - **LAN1 Subnet Mask** — <subnet mask appropriate for the subnet of which this bridge is a member>
  - **LAN1 Gateway** — (Leave empty)
- 6 On the **Quick Setup** menu, fill in the **LAN2 (untrusted)** fields as described below:
  - **LAN2 Configure IP** — automatic-via-DHCP
  - **LAN2 IP Address** — (Leave empty)
  - **LAN2 Subnet Mask** — (Leave empty)
  - **LAN2 Gateway** — (Leave empty)

**PROCEDURE 1-4** HOW TO CONFIGURE THE CLIENT-SIDE UT-3302 BRIDGE (CONTINUED)

- 7 On the **Quick Setup** menu, fill in the **Ethernet Tunnel** fields as described below:
- **Shared Secret** — *<secret phrase that must be the same on client and server bridges, can be up to 52 characters, no quote or backslash>*
  - **Encryption** — 128 bit, 192 bit, or 256 bit AES  
*Encryption setting must be the same on client and server bridges.*
  - **Mode** — client
  - **Authorized Client Name1** — (Leave empty)
  - **Authorized Client Password1** — (Leave empty)
  - **Server Port** — (Leave empty)
  - **Client Name** — *<user name that must be the same as **Authorized Client Name1** on server bridge, can be up to 52 characters, no quote or backslash>*
  - **Client Password** — *<user password that must be the same as **Authorized Client Password1** on server bridge, can be up to 52 characters, no quote or backslash>*
  - **Remote Server IP** — *<LAN2 (untrusted) IP address of the server-side UT-3302 bridge>*

**NOTE**

For **Remote Server IP**, use the IP address noted in step 9 of Procedure 1-2.

- **Remote Server Port** — *<server port used by server-side UT-3302 bridge; default is 22>*
- **Interface** — Lan2 (accept the default)

- 8 Click **Store & Activate**.

**Result:** The new settings are saved and made active.

## CLIENT-SIDE UT-3302 INSTALLATION

Install the client-side UT-3302 bridge.

### PROCEDURE 1-5 HOW TO INSTALL THE CLIENT-SIDE UT-3302 BRIDGE

- 1** If it is not already connected, connect the Untrusted port of the UT-3302 bridge directly to the Internet connection provided by the Internet service provider at the remote location.
- 2** Connect one of the Trusted ports of the UT-3302 bridge to the Ethernet port of the remote console computer.  
**Result:** The UT-3302 bridge is inserted between the remote MIP 5000 console and the Internet.
- 3** Power up the UT-3302 bridge and the other equipment.

## REMOTE CONSOLE NETWORK CONFIGURATION

Configure the client-side network to be part of the dispatch center subnet.

### PROCEDURE 1-6 HOW TO CONFIGURE THE CLIENT-SIDE NETWORK

- 1** Change the IP address of remote console computer to the one assigned at step 1 of Procedure 1-3.



#### EXAMPLE

In Figure 1-3, “Example MIP 5000 VPN Connection,” the IP address used is 192.168.0.110.

- 2** Plug in all necessary USB jackboxes, headsets, speakers, and microphones.
- 3** Start the MIP 5000 VoIP Radio Console program and log in.  
**Result:** You are connected to the MIP 5000 resources at the dispatch center and you can start dispatching.

**THIS PAGE INTENTIONALLY LEFT BLANK.**

# GLOSSARY

---

**AES** — Advanced Encryption Standard, a set of encryption standards adopted by the U.S. government. It is a highly effective method of preventing data from being interpreted by unintended recipients.

**Ethernet** — A family of frame-based protocols for transmitting data between entities on a network.

**ISP** — Internet Service Provider, an organization that provides access to the Internet.

**Kbps** — Kilobits per second (1024 bits per second).

**Mbps** — Megabits per second (1,048,576 bits per second).

**VPN** — Virtual private network, a method of encapsulating data that traverses a public network so that the data is kept private and unavailable to entities on the public network.

**THIS PAGE INTENTIONALLY LEFT BLANK.**

# INDEX

.....

## B

.....  
 bandwidth requirements .....1-2

## C

.....  
 configuration ..... remote console network .....1-15

## D

.....  
 data transfer rate requirements .....1-2      dispatch center setup .....1-5

## M

.....  
 MIP 5000 documentation ..... x

## P

.....  
 prerequisites .....1-4      remote console site .....1-4  
     dispatch center .....1-4

## R

.....  
 recommendations .....1-3      remote console preparation .....1-11  
 references ..... x      remote console setup .....1-10  
 related information ..... x      requirements  
 remote console network configuration .....1-15           throughput .....1-2

## S

.....  
 setup ..... single subnet .....1-3  
     dispatch center .....1-5  
     remote console site .....1-10

**T**

.....  
throughput requirements..... 1-2

**U**

.....  
UT-3302 configuration  
    client-side..... 1-13  
    server-side..... 1-7

.....  
UT-3302 installation  
    client-side..... 1-15  
    server-side..... 1-6





MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. All other product or service names are the property of their respective owners.

© Motorola, Inc. 2009. All rights reserved.

2215247G-01