FIAL INCORPORATED

MCS-11/IP TUNNEL

MODELS 2701 AND 2705

FIAL INCORPORATED
4343 SW CORBETT AVE.
PORTLAND, OR 97239
503.227.7083
WWW.FIAL.COM

Document Number 2701/5-030320

TABLE OF CONTENTS

INTRODUCTION:

The IP Tunnel is a tool designed to bridge communication gaps that occur when non-MCS-11 radios are added to (or replace portion(s) of) MCS-11 radios. With the IP Tunnel, MCS-11 (usually poll and response) packets are wrapped up by the IP Tunnel device in an IP Ethernet packet and sent using the Internet to another IP Tunnel device, which receives the IP Ethernet packets, unwraps them, and delivers them to the correct MCS-11 address.

A minimum of two IP Tunnel devices (one Server and one Client,) are required, one at each end of an IP link. Each device accepts MCS-11 traffic through its MCS-11 port, wraps the traffic in an IP packet and transports the traffic to the second device through its Ethernet LAN port. Upon receiving the packet, the second IP Tunnel device unwraps the IP packet and forwards the MCS-11 traffic to the appropriate MCS-11 device.

Each IP Tunnel installation has at least one device designated as a "Server," and at least one device designated as a "Client." Each Server IP Tunnel device can communicate with up to 64 Client devices. Large MCS-11 networks may gain a speed advantage by splitting up the remote MCS-11 addresses (or IP tunnel Clients) between two or more IP Tunnel Servers, connecting each to its own Polling Engine port. This allows simultaneous polling. This option is not available if the MCS-11 network is a ring (i.e. using an AE36S-2 or 2602 polling engine).

Any IP Tunnel device may be configured to be a "Server" or "Client." (For more information, refer to Configuring Your IP Tunnel Device on page 3).

How The IP Tunnel Works

CONNECTIVITY

IP Tunnel devices have at least three ports: a Craft port, a LAN (Ethernet/IP) port and an MCS-11 port. The 2701 has one MCS-11 port. The 2705 has five MCS-11 ports.

In a typical application, a Server IP Tunnel device is connected to an MCS-11 Polling Engine or Bridge using its MCS-11 port, and also to an IP network using its Ethernet port. The Client IP Tunnel devices are also installed and similarly connected elsewhere on the IP network near remote MCS-11 devices such as Alcatel™ microwave radios or switches.

The Server is provisioned with the IP address and a list of MCS-11 addresses for each Client. The Server can communicate with a polling engine's MCS-11 port, and with multiple Client IP Tunnel devices through its IP port as shown in Figure 1. Similarly, the Client IP Tunnel devices can also communicate with their Server and MCS-11 radios using their ports.

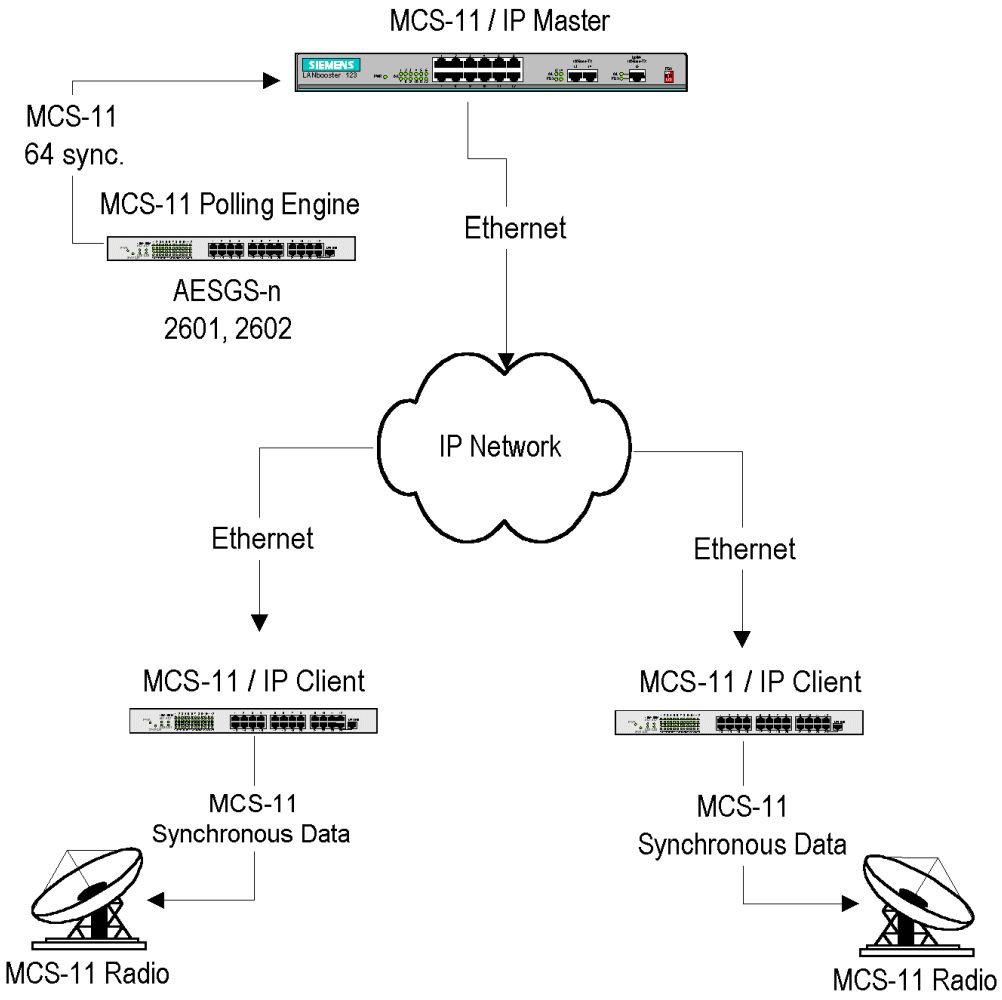


Figure 1. IP Tunnel Connectivity

Server Operation

When the Server receives a poll from a Polling Engine, it consults its tables of Client MCS-11 addresses to find a match. It then wraps the MCS-11 poll in an IP packet, and forwards the message to the proper Client via its LAN connection. If the Server cannot find an MCS-11 address match, it discards the poll. When the Server receives an IP packet from a Client, it extracts the MCS-11 response and forwards it to the Polling Engine via its MCS-11 port. Typically, the response packet will be an MCS-11 polling response.

Client Operation

When an IP packet from an IP Tunnel Server arrives at an IP Tunnel Client, the Client extracts the MCS-11 packet and sends it out its MCS-11 port. Typically, this packet will be an MCS-11 poll. When an MCS-11 response arrives, the Client wraps it in an IP packet and forwards it to the Server that requested it.

CONFIGURING YOUR IP TUNNEL DEVICE

Every IP Tunnel device must be configured before it is installed at its physical location. A default IP address (192.168.1.200) is present in each IP Tunnel device shipped from the factory; however, you must set the actual IP address that each device (Server or Client) will use in your network. In addition, you must configure the settings for each device to define Server or Client operation, as well as the MCS-11 addresses assigned to each client.

The IP Tunnel may be provisioned two ways:

1. Use the rear-panel serial (craft) interface port with a terminal emulation program.

2. Use the LAN (Ethernet) port and a web browser to connect locally or remotely to the IP Tunnel's built-in web server.

Note: The craft interface screens are also accessible remotely via a telnet connection.

The web page configuration has an Undo All Changes feature not supported in the more simple craft interface. However, all steps necessary to provision an IP Tunnel device are available using the craft port (or telnet) connection.

The craft port is always accessible for changing the IP settings. The web interface is not accessible if you do not know the device's current IP settings. The web interface is easier to use (see Initial Configuration With A Web Browser on page 9).

Configuring With The Craft Serial Port

The Craft (serial) port interface provides a direct connection (straight through cable) to a PC COM port. Connect to the Craft port of the IP Tunnel device with a terminal program (such as HyperTerminal), and provision the default IP address for the device (192.168.1.200). Set HyperTerminal to 9600 baud, 8-data bits, no-parity and 1-stop bit. Power up the IP Tunnel device. After a few seconds, the login prompt will appear (see Figure 2).

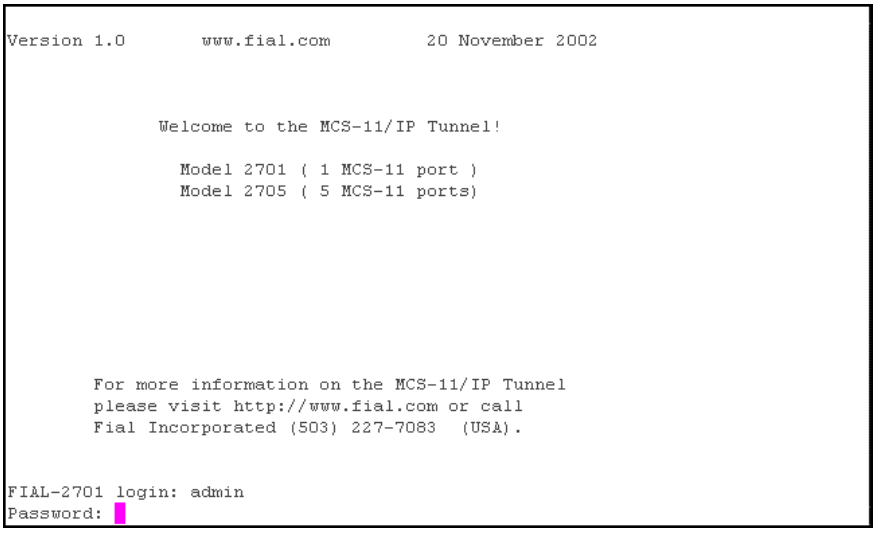


Figure 2. Craft Port Login Window

Login with User Name **admin** and Password **tunnel**. The Main Menu will appear.

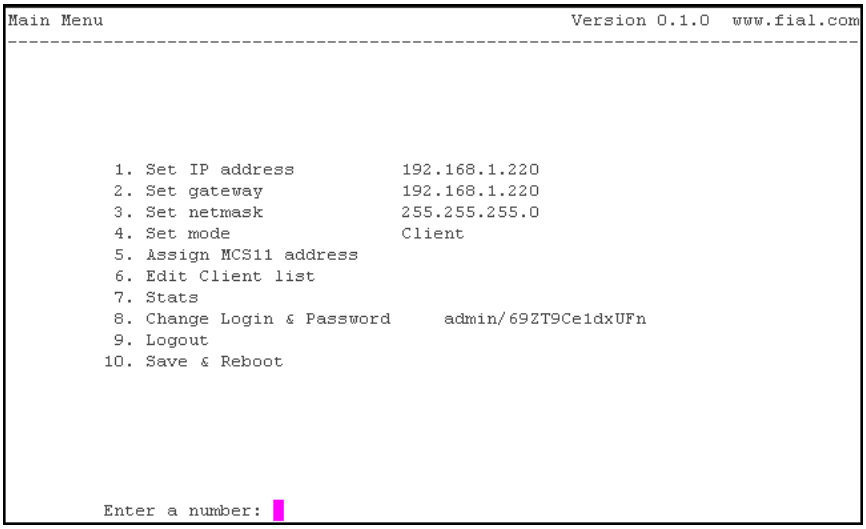


Figure 3. Main Menu

The Main Menu window has a list of 10 options for configuring the IP Tunnel device. To configure the device, complete the following steps:

1. Set the IP Address

To set a new IP Address for your IP Tunnel device, select 1 and press enter. The Set IP Address window will appear.

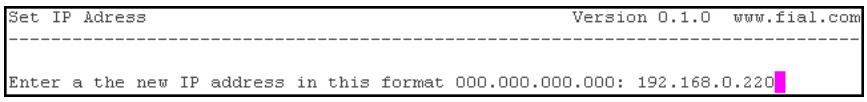


Figure 4. Set IP Address Via HyperTerminal

After the prompt, enter the new IP address and press return.

NOTE: Do not select option 10 (Save & Reboot) until you have made any other changes for the device and verified them. Doing otherwise may render the device inaccessible from the LAN (See IP Addresses on page 23 for IP address restrictions). In many cases, you will provision a Server using the factory default IP address, then as a last step change the IP address, netmask and gateway, followed by a save-and-reboot. At this point you may lose IP access to the device, although the device is now ready to be installed in the proper address zone.

2. Set the Gateway

To set the new gateway for the IP Tunnel device, select option 2 and press return. The Set Gateway window will appear.

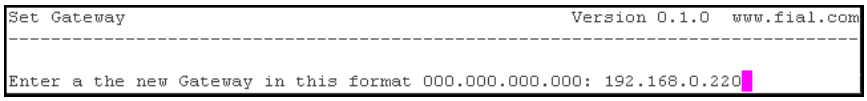


Figure 5. Set Gateway Via HyperTerminal

After the prompt, enter the Gateway and press return.

NOTE: Do not select option 10 (Save & Reboot) until you have made any other changes for the device and verified them. Doing otherwise may render the device inaccessible from LAN. (See IP Addresses on page 23 for IP address restrictions).

3. Set the Netmask

To set the new netmask for the IP Tunnel device, select option 3 and press return. The Set netmask window will appear.

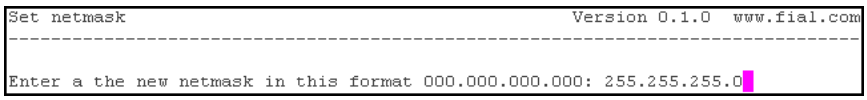


Figure 6. Set Netmask Via Craft Screens

After the prompt, enter the netmask and press return.

NOTE: Do not select option 10 (Save & Reboot) until you have made any other changes for the device and verified them. Doing otherwise may render the device

inaccessible from the LAN. (See IP Addresses on page 23 for IP address restrictions).

4. Set Mode

To select a mode (Server vs. Client) for the IP Tunnel device, select option 4 and press return. The Set mode window will appear.

```
Set mode                                                    Version 0.1.0  www.fial.com
--------------------------------------------------------------------------------

    1) CLient

    2) Server


Enter 1 or 2: 1
```

Figure 7. Set Mode Via Craft Screens

After the prompt, enter 1 if this device will be a Client, or 2 if this device will be a Server, and press return.

5. Assign MCS-11 Addresses (if device is to be a Server)

To assign the MCS-11 addresses for which an IP Tunnel Server has communication responsibility, select option 5 and press return. The Assign MCS-11 Address window will appear.

```
Assign MCS11 address                                    Version 0.1.0  www.fial.com
--------------------------------------------------------------------------------

   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10| 11| 12| 13| 14| 15| 16|
 ---------------------------------------------------------------------
 A |  1|  1|  1|  1|  1|  1|  1|  1|  1|  1|  1|  1|  1|  1|  1|  1|
 B |  0|  0|  0|  0|  0|  0|  0|  2|  2|  2|  2|  2|  2|  2|  2|  2|
 C |  3|  3|  3|  3|  3|  3|  3|  0|  0|  0|  0|  0|  0|  0|  0|  0|
 D |  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|
 E |  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|
 F |  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|
 G |  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|
 H |  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|  0|

 1-Salem            2-Portland          3-Eugene            4-Beaverton
 5-                 6-                  7-                  8-
 9-                10-                 11-                 12-
13-                14-                 15-                 16-
17-                18-                 19-                 20-
21-                22-                 23-                 24-
25-                26-                 27-                 28-
29-                30-                 31-                 32-

Enter the number of client to assign or press return for more: 4
Enter the address range or press return for menu (ex: A,1,16): d,1,16
```

Figure 8. Assign MCS-11 Addresses

The Assign MCS-11 Address window has 2 tables displayed on the screen. The first table shows the MCS-11 addresses and the Clients to which they are mapped. In this table, Clients are represented by a client number. The following (second) table displays Client numbers in conjunction with their Client names.

The Server uses these tables to look up all MCS-11 requests for a given address, puts them in an IP packet, and sends them to the mapped IP address. If an MCS-11 address is not mapped to a Client number, the MCS-11 packet will be ignored.

To map MCS-11 addresses, enter the number of the Client to which the address range will be assigned and press enter. Then enter the MCS-11 address range. The example given is “A,1,16” which would map MCS-11 addresses A1 thru A16 to the selected Client.

To clear an address range, assign the address range to Client number 0 (which does not ever exist).

6. Edit Client List

The Edit Client window is only available if this IP Tunnel device has been provisioned as a Server. Using the Edit Client window, you may add or change each Client's name and IP address.

To edit the Client list for this IP Tunnel device Server, select option 6 and press return. The Edit Client window will appear.

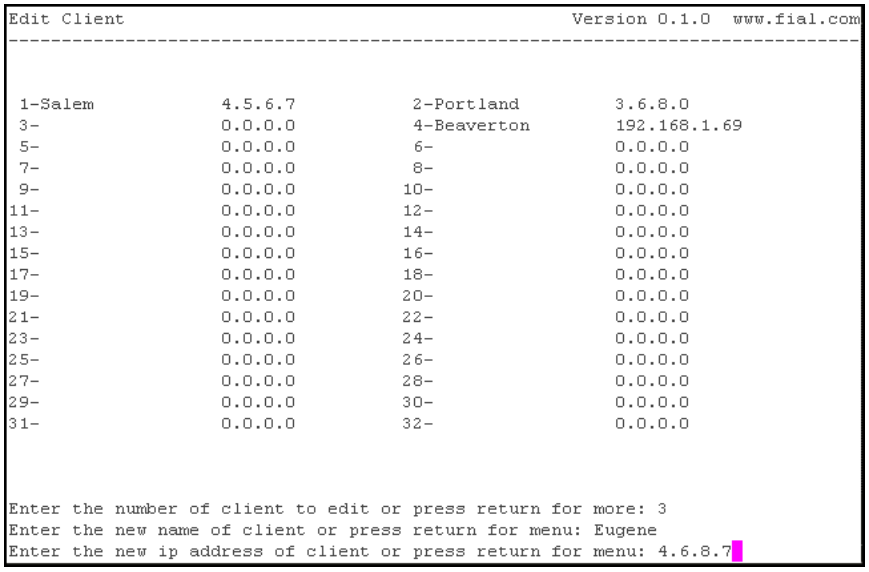


Figure 9. Edit Clients Via Craft Screens

The Client list is the list of clients to which the Server will send Ethernet IP packets. A Client must be added to this list before it can be mapped to an MCS-11 address range.

To edit Client properties, type the Client number and press enter. Type the Client name, press enter, then type the IP address and press enter. If you press enter without changing a field, the current contents will be unchanged. Note that A-Z, a-z, 0-9, and hyphen are the only characters allowed in the Client name.

The client name is for operator convenience only. It allows keeping track of clients by name instead of cryptic IP addresses. The client name is not used for name resolution (that is, converting a client name to an IP address). You may find it useful to add server and client names with corresponding IP addresses to your DNS server. That will allow you to connect to the unit using a host name instead of an IP address.

To delete a client, choose the client number you wish to delete and press enter. Then type "delete" for the client name and press enter. The client will be removed from the list.

7. Edit Stats

The Stats window shows the health of the IP Tunnel device. To view the Stats window, select option 7 and press return. The Stats window will appear.

```
Stats                                                       Version 0.1.0  www.fial.com
-----------------------------------------------------------------------------------------

Client Name       UDP      UDP      UDP      UDP      MCS      MCS      MCS     Invalid
                  tx       rx       lostout  lostin   norep    late     Out/Ord Poll
-----------------------------------------------------------------------------------------
Salem             0        0        0        0        0        0        0       0
Portland          0        0        0        0        0        0        0       0
Eugene            0        0        0        0        0        0        0       0
Beaverton         0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0
                  0        0        0        0        0        0        0       0

Press return for more:
```

Figure 10. Stats Via Craft Screens

8. Change Login & Password

Each IP Tunnel device has a default Login (admin) and Password (tunnel) programmed at the factory. Remember that both the login and password are case sensitive. Any user with the correct Login and Password will have access to the Craft port of the device and web page configurations. For security purposes, it is recommended that the Login and Password for each device be changed during the initial configuration. If you forget the new login and password or are unable to login to the device, the login and password can be reset to the factory default by holding down the lamp test button while the device is restarted (reset). You must hold down the button for approximately 15 seconds. No other provisioning will be affected.

To change the login and password for an IP Tunnel device, select option 8 and press return. The Set Login & Password window will appear.

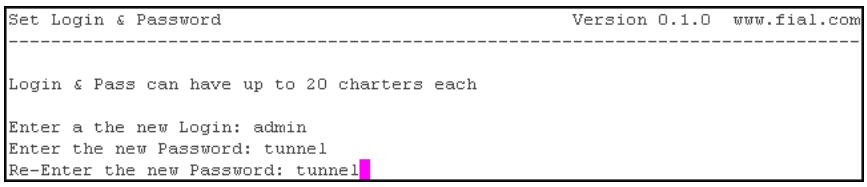


Figure 11. Set Login & Password Via Craft Screens

To change the Login and Password, follow the prompts: enter the new Login, enter the new Password, and re-enter the new password. Remember that both the Login and Password are case sensitive. A-Z, a-z, 0-9, and hyphen are the only characters allowed for the Login. The password can be any combination of charters, numbers and special characters. Passwords should be longer than 8 characters in length. For more information, refer to Login & Password in the Notes section on page 24.

9. Logout

To log out of the IP Tunnel device configuration session, type 9 and press return. If you are connected through telnet, Logout will close your telnet connection. If you are using HyperTerminal you will be logged out of the device and presented with the login screens.

NOTE: Before logging out, select 10: Save & Reboot. Doing otherwise will cause all changes to be erased.

10. Save & Reboot

After all changes have been made for the IP Tunnel device, choose Save & Reboot. This will save your changes, and the device will restart with the new settings. If you do not choose Save & Reboot, any changes made in this login session will not take effect. For detailed information on Save & Reboot versus Submit, refer to the section Save & Reboot on page 19.

Initial Configuration With A Web Browser

To provision an IP Tunnel device using a web browser, connect the IP Tunnel to a laptop (or PC) with a 10BaseT Crossover cable, or connect both your laptop and the IP Tunnel to a hub or a switch. (The laptop should have Microsoft Internet Explorer web browser 5.0 or later or Netscape 7.0 as a default web browser. For Netscape 7.0, verify that **Enable JavaScript for Navigator** is "checked" in the Edit/Preferences/Advanced/Scripts & Plugins/Verify device).

Set your computer to an IP address in the range of 192.168.1.2 to 192.168.1.253, and netmask to 255.255.255.0. Set your gateway address to match the IP address that you set above. (Do NOT use IP address 192.168.1.200; this is the IP Tunnel factory default address). For example, set your IP address to 192.168.1.10, your netmask to 255.255.255.0, and your gateway to 192.168.1.10.

Since this is the initial configuration for the IP Tunnel, enter http://192.168.1.200 into the browser URL (address) device and press Enter. The Master MCS-11/IP Tunnel window will appear. (See Figure 12).

Warning: When you change the IP address, gateway and netmask using the web browser interface, you may lose your IP connectivity with the device. This will happen when you choose Save and Reboot. You may then need to change your laptop (or PC) IP settings to access the IP Tunnel device's web server.

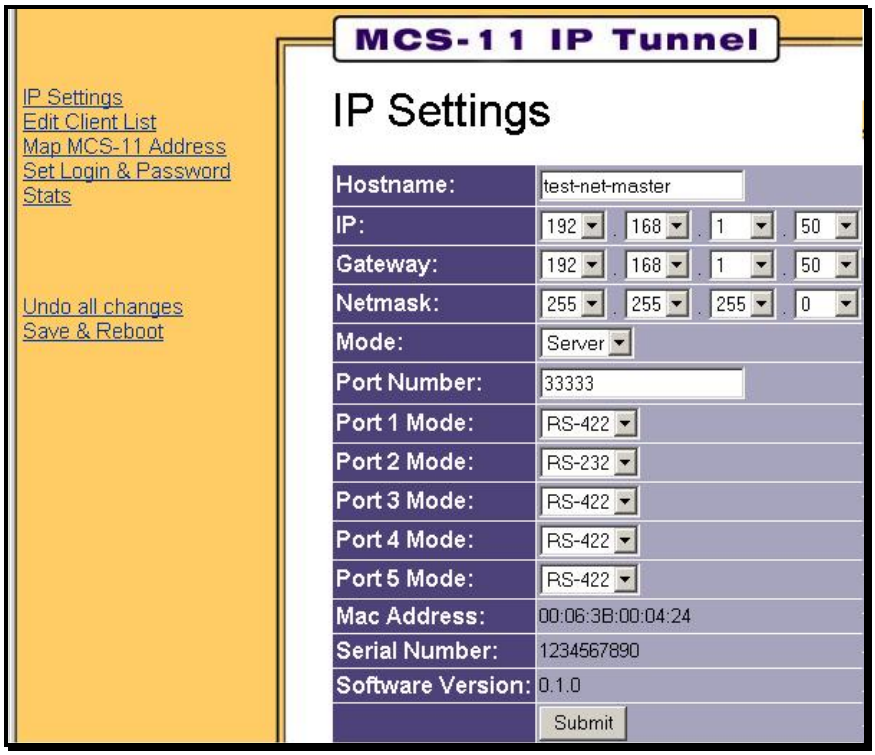


Figure 12. The Master Window

The Master window displays the current settings for the IP Tunnel device. Values are for display only, and may not be changed without first selecting a menu item in the left pane.

The left pane of the Master Window has links to other windows such as Client List, MCS-11 Address and Stats windows. Based on whether the current mode of the IP Tunnel device is set to "Server" or "Client," menu items in the left pane will vary. For example, if "Client" is selected, links for *Edit Client List*, *Map MCS-11 Addresses* and *Stats*, will disappear.

To modify the IP Tunnel device settings, click on the hot links in the left pane. Remember, to activate any changes, you must click the Submit button on any screens you change and choose Save & Reboot when you are done.

THE IP SETTINGS WINDOW

The IP settings and Server versus Client operation are provisioned in the IP Settings window. To make changes, first click on IP Settings in the left pane. An Enter Network Password window will prompt you to enter a User Name and Password for the IP Tunnel device.

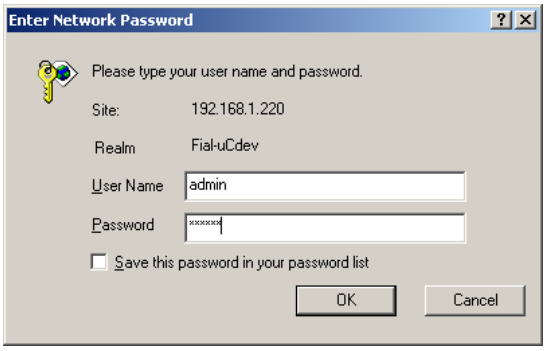


Figure 13. Enter Network Password Via The Web

If this is the first time the device has been provisioned, enter the factory set user name (**admin)** and password (**tunnel)** in the fields and click OK. Otherwise, enter the updated user name and password in the appropriate fields, and click OK. The IP Settings window will now allow you to modify values for the IP Tunnel device. For other login issues, refer to Login & Password in the Notes section.

Enter new values for the following fields on the right-hand pane:

Hostname: Enter an arbitrary host name for the device. A - Z, a - z, 0 - 9, and hyphen are the only characters allowed.

IP: Enter the IP address for this device by clicking on the drop-down boxes and selecting a number for each field. (See IP Addresses on page 23 for IP address restrictions).

The default IP address for every IP Tunnel device is 192.168.1.200. At a minimum, you must change the last three digits of the IP Address for all subsequent boxes. (Example: 192.168.1.201).

The IP Address of a *Client* IP Tunnel device may be modified using the web at a later date by accessing the IP Tunnel Server and assigning a new IP address for the Client. However, connection to the Client itself may be lost if you set an IP address that you cannot reach.

NOTE: Do not "Save & Reboot" after changing the IP address, Netmask or Gateway, until you have made all other changes and verified them. Doing otherwise may render the device inaccessible to you as a result of an IP settings change.

Gateway - Enter the gateway IP address for this device. Packets will be sent to the gateway if the destination IP address does not match the IP address range (zone) for the device. The gateway is usually a router that sends IP packets to their proper destination.

NOTE: Do not "Save & Reboot" after changing the IP address, Netmask or Gateway, until you have made all other changes and verified them. Doing otherwise may render the device inaccessible to you.

Netmask - Enter the netmask for the device. The IP address and netmask are closely linked, and must be determined by an IP network administrator or someone familiar with the IP address mappings for the sites on your local area network (LAN). See NOTE 2 below for additional netmask information.

NOTE: Do not "Save & Reboot" after changing the IP address, Netmask or Gateway, until you have made all other changes and verified them. Doing otherwise may render the device inaccessible to you.

Mode - Select the Server or Client status for this device from the Mode drop down menu. If Client is selected, the left pane links for *Edit Client List*, *Map MCS-11 Addresses* and *Stats* (statistics) will no longer be visible.

Port Number - Enter the port number to be used by the Server and its associated Clients. All IP Tunnel devices are pre-configured to port number 33333. Valid numbers are 1 to 65535. The same port number must be used for a Server and all of its Clients.

NOTE: Do not use port numbers below 5000. These port numbers are used by IP services, and are often blocked by firewalls.

Port # Mode - Select *RS-422* (factory default) or *RS-232* operation for each MCS-11 port. (For *important* information on RS-422, RS-232 and port numbers, see RS 232 and RS 422 in the Notes section on page 25.) An L.E.D. on the rear panel indicates RS-422 LED ON) or RS-232 (LED OFF) for each MCS-11 port.

Mac Address - All IP Tunnel devices contain a factory-assigned Mac Address. The Media Access Control (MAC) address is the network card address for the Ethernet port. It is a unique number, different for every network card ever manufactured and thus, cannot be changed.

Serial Number - The serial number displays the factory serial number for the device. This number cannot be changed.

Software Version - The software version number identifies the release or build version of the software installed in the device. This number cannot be changed.

Click The Submit Button

Once all changes have been made, press the Submit button. This button must be pressed to register any changes made on this screen. Changes are temporarily stored in a file on the device, and are keyed to your IP address. To actually *install* the changes, the "Save & Reboot" link on the left pane must be selected, and you must confirm the request by clicking YES when prompted. This software design allows you to make changes on different screens, submit the changes before you leave the screens, and choose "Save & Reboot" just once at the end. If you do not choose "Save & Reboot," your submitted changes will be erased after a few hours of inactivity. (For detailed information on Save & Reboot versus Submit, refer to the section Save & Reboot on page 19).

THE EDIT CLIENT LIST WINDOW

Each Server requires at least one Client with which to communicate. To add a Client or modify the Server Client list, click the Edit Client List link in the left pane. (This link is only visible when a Server has been selected in the IP Settings window. If this link is not visible, go back to the IP Settings window and verify that "Client" has not been selected in the Mode box).

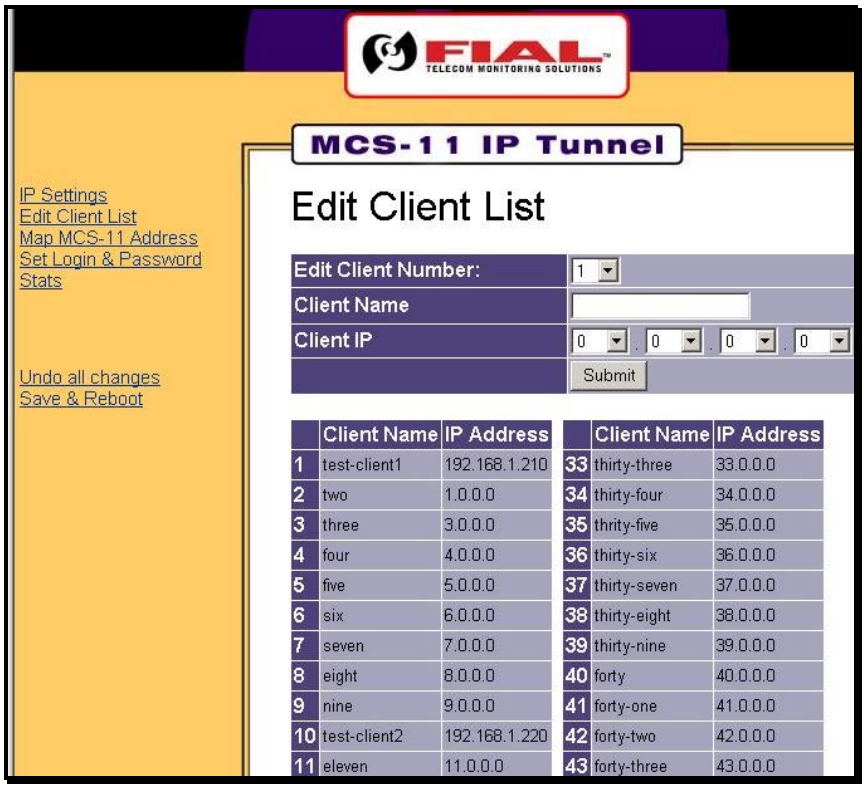


Figure 14. Edit Client List Window Via The Web

The Edit Client List window (as shown in Figure 14), displays a table that lists the Clients to which the Server will send IP Ethernet packets. Client information includes a Client number and an IP Address.

Up to 64 Clients can be assigned to every Server. Each Client will have a name (not necessarily unique), and an IP address that MUST be unique. To add a Client, edit the following fields:

Edit Client Number: To add a Client, choose a number from the client list with blank name and IP address. Enter that number in the Edit Client Number drop-down list. To modify a Client, select the number from the drop-down menu for the Client that you wish to change.

Client Name: If this is a new Client, enter a name for the selected Client. (A-Z, a-z, 0-9, and hyphen are the only characters allowed). The Client name is for operator convenience only. It allows viewing a Client by name instead of IP address or number. Client names can be the same as other Clients; however, this is not recommended for obvious reasons. The Client name is not used for name resolution (that is, converting a client name to an IP address).

Client IP: Enter the IP address for this Client. Click on the drop-down boxes and select the appropriate numbers.

Deleting a Client

There may be times when a Client needs to be deleted from the Server list. There are two ways to accomplish this. The first way is to select the Client number that you wish to delete from the Client drop-down list, erase the Client name box, set the IP address to 0.0.0.0. and click on the Submit button.

The second way is to use the "Delete Client Number" drop down box at the bottom of the page to select the number of the Client you wish to delete (see Figure 15), and press the Delete button. You will be asked to confirm the request by clicking "YES."

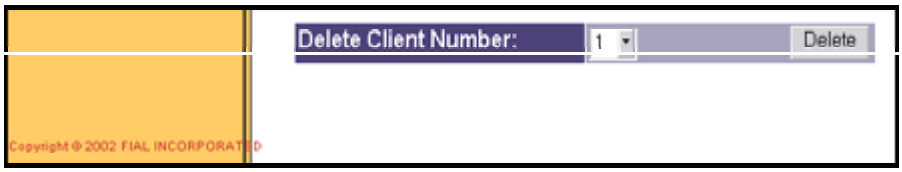


Figure 15. Deleting A Client Via The Web

Click The Submit Button

After all changes have been made, press the Submit button. This button must be pressed to register any changes made on this screen. To actually *install* the changes and put them in effect, click the "Save & Reboot" link on the left pane and confirm the request by clicking YES when prompted. (For detailed information on Save & Reboot versus Submit, refer to the section Save & Reboot on page 19).

THE MAP MCS-11 ADDRESS WINDOW

After a Client has been created in the Edit Client List window, MCS-11 addresses must be assigned to it. To view MCS-11 addresses assigned to a Client, or map an MCS-11 address range to a Client, click on the Map MCS-11 Address link in the left pane. The Map MCS-11 Address window will appear, as shown in Figure 16. (This link is only visible when Server device mode has been selected in the IP Settings window. If the MAP MCS-11 Address link is not visible, go back to the IP Settings window and verify that "Client" has not been selected in the Mode box).

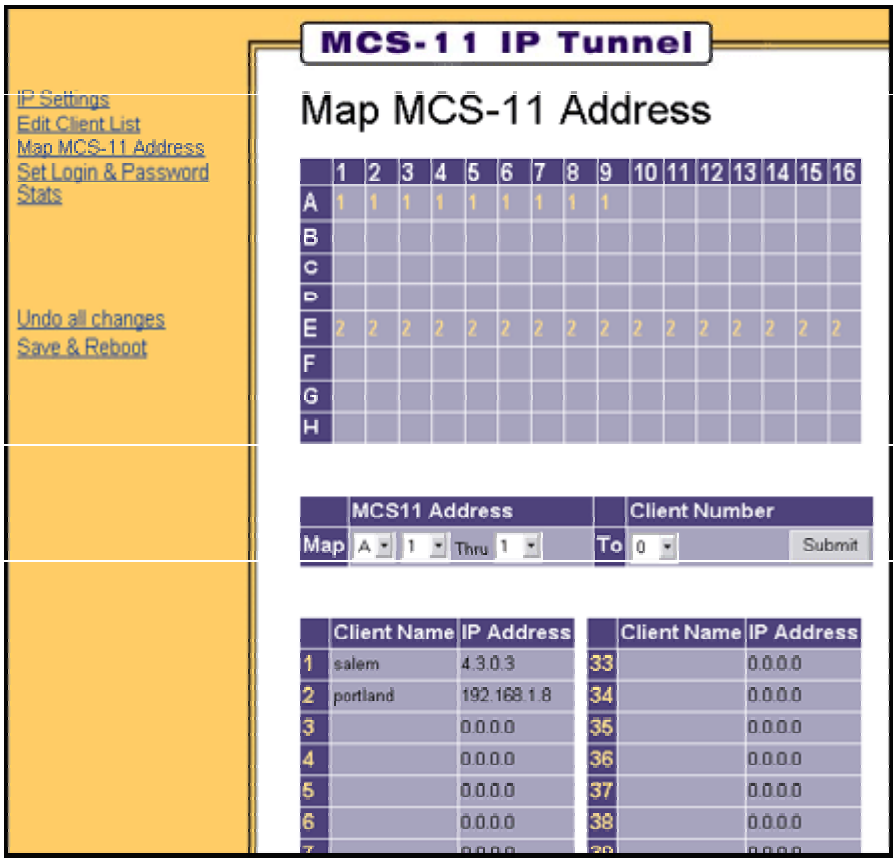


Figure 16. Map MCS-11 Address Via The Web

The Map MCS-11 Address window displays two tables. The first table displays MCS-11 addresses and the Clients to which they are mapped. Clients are represented by a Client number. To find the Client's individual name and IP address, look at the second table and match the number from the top table to the number in the bottom table.

The IP Tunnel Server uses these two tables to determine where to send an MCS-11 packet request before putting the packet in an Ethernet IP packet and sending it to the mapped IP address. If an MCS-11 address is not mapped to a client number, MCS-11 packets with that address will be ignored.

To assign additional MCS-11 addresses to a Client (number), complete the following fields:

MCS11 Address:

Map: Enter or select the starting address in the MCS-11 address range from the first two drop-down fields. The first drop-down box represents the alphabet part of the address, while the second is for the numeric part. (Only one alphabet range can be mapped at a time).
Thru: Select the ending number in the MCS-11 address range from the drop-down box.

To map a single MCS-11 address to a Client number, enter the same number in the MCS-11 address in the Map and Thru fields. For example, to map A5 only to Client 2, enter Map A5 Thru 5 to Client 2, then press the Submit button.

To clear a set of MCS-11 addresses, use the above method to select the starting and ending address and select Client number 0. Then press the Submit button.

Client Number: Select the number of the Client that will handle this range of MCS-11 addresses, from the drop-down menu. MCS-11 polls for these addresses will be sent to the Client specified. (If you cannot remember the Client's number, reference the second table in this window to view a list of Client Names and numbers).

Click The Submit Button

After all changes have been made, press the Submit button. This button must be pressed to register any changes made on this screen. To actually *install* the changes, click the "Save & Reboot" link on the left pane and confirm the request by clicking YES when prompted. (For detailed information on Save & Reboot versus Submit, refer to the section Save & Reboot on page 19).

SET LOGIN & PASSWORD

For security purposes, it is recommended that the Login and Password for each device be changed from the factory default **admin** and **tunnel**, during the initial configuration. Any user with the correct Login and Password will have access to the Craft port of the device (also reachable via telnet), and web page configuration screens.

To change the login and password for an IP Tunnel device, click the Set Login & Password link in the left pane.

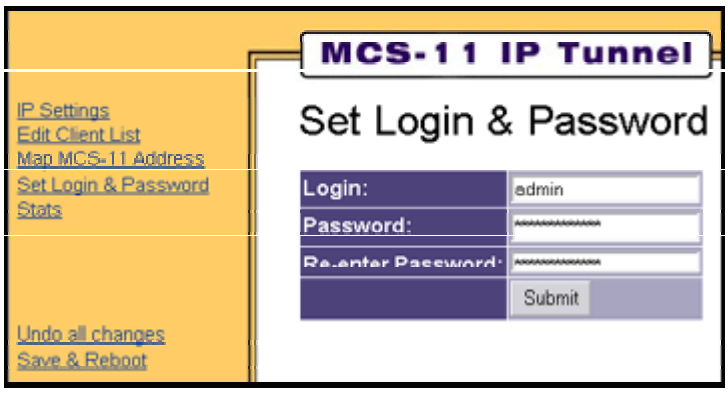


Figure 17. Set Login & Password Via The Web

The Set Login & Password window will prompt you to change the login password for the device. To change the Login and Password, complete the following fields:

Login: Enter the new Login name for the device.

Password: Enter the new Password for the device.

Re-enter Password: Re-enter the new Password for the device.

Remember that both the Login and Password are case sensitive. A-Z, a-z, 0-9, and hyphen are the only characters allowed for the Login. The password can be any combination of characters, numbers and special characters. Passwords should be longer than 8 characters in length. For more information, refer to Login & Password in the Notes section on page 24.

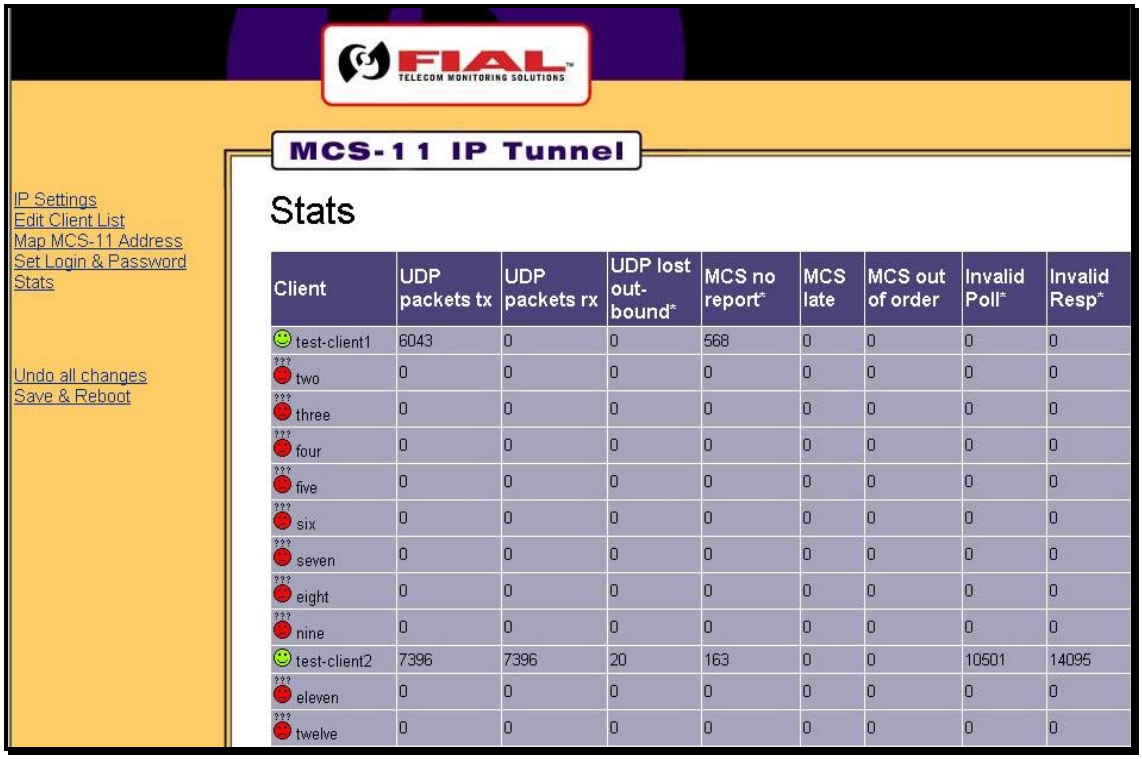
Click The Submit Button

After all changes have been made, press the Submit button. This button must be pressed to register any changes made on this screen. To actually *install* the changes, click the "Save & Reboot" link on the left pane and confirm the request by clicking YES when prompted. (For detailed information, refer to the section Save & Reboot on page 19).

THE STATS WINDOW

The Stats (statistics) window is a detailed table that displays the health of the IP Tunnel device. The Stats table is only maintained in IP Tunnel Servers.

To access the Stats window, click on "Stats" in the left pane. (This link is only visible when a Server has been selected in the IP Settings window. If this link is not visible, go back to the IP Settings window and verify that "Client" has not been selected in the Mode box). The Stats window will appear. (See Figure 18).



Client	UDP packets tx	UDP packets rx	UDP lost out-bound*	MCS no report*	MCS late	MCS out of order	Invalid Poll*	Invalid Resp*
test-client1	6043	0	0	568	0	0	0	0
two	0	0	0	0	0	0	0	0
three	0	0	0	0	0	0	0	0
four	0	0	0	0	0	0	0	0
five	0	0	0	0	0	0	0	0
six	0	0	0	0	0	0	0	0
seven	0	0	0	0	0	0	0	0
eight	0	0	0	0	0	0	0	0
nine	0	0	0	0	0	0	0	0
test-client2	7396	7396	20	163	0	0	10501	14095
eleven	0	0	0	0	0	0	0	0
twelve	0	0	0	0	0	0	0	0

Figure 18. Stats Via The Web

The columns in the Stats window are explained in a table at the bottom of the Stats window (see Figure 19).

Green Smiley:	Server is receiving IP/UDP packets containing MCS-11 responses or error statistics from the client.
Red Smiley:	Server has not had any IP/UDP contact with the client in the last 30 seconds, and client did not respond to a 'statistics' request.
UDP packets tx:	Number of IP/UDP poll packets the server sent to the client.
UDP packets rx:	Number of IP/UDP response packets the server received from the client. Will be much lower than tx if client has many MCS no-reports.
UDP lost outbound:	Number of IP/UDP packets the client did not receive. Client counts missing poll-packet sequence numbers, sends 'missed' count back to server.
MCS no report:	Client received next IP/UDP poll while still was waiting for an MCS-11 answer to a previous poll.
MCS late:	Server received a IP/UDP packet with correct MCS-11 response address. But the MCS-11 answer is from a previous poll.
MCS out of order:	Server received an IP/UDP packet with an MCS-11 answer but was not waiting for an answer from this MCS-11 address.
Invalid poll:	Client received an MCS-11 poll on its physical MCS-11 interface. The client should never receive MCS-11 polls from MCS-11 remotes.
Invalid response:	Client received an MCS-11 response, but no poll was sent for that MCS-11 address.
Wrong MCS address:	Client received an MCS-11 response but was waiting for a response from a different MCS-11 address.
	* Denotes a count generated by client. Client counts are sent back to the server in each response packet. Client statistics will not be current if a red smiley is present. Server sends a 'statistics request' to client if client has sent no UDP/IP responses for over 30 seconds.

Figure 19. The Stats Window Definition Table

UNDO ALL CHANGES

At times, you may wish to undo configuration changes already submitted (such as during a training session) throughout the IP Tunnel windows. To undo these changes and revert to the last saved settings, click the Undo All Changes link in the left pane. This will only work on changes submitted in this login session, as long as you have not clicked the "Save & Reboot" button.

SAVE & REBOOT

After all changes have been made, press the "Save & Reboot" link in the left pane. This link installs all of the temporary changes stored when the Submit button was pressed. Confirm the request by clicking YES when prompted.

If you do not choose "Save & Reboot," any submitted changes will be erased after a few hours of inactivity.

Note: If two people are editing the configuration of the same IP Tunnel device at the same time, the first one to "Save & Reboot" will have their changes applied. Any changes made by the second user will be lost, and the second user will have to log in again and start over.

HARDWARE SETUP

The IP Tunnel device is connected to the IP network using an Ethernet RJ45 jack and standard 10BaseT or 100BaseT wiring. The device connects to MCS-11 equipment with the standard DB15 connector. Older equipment may require a 20-pin IDC connector at the equipment end. The MCS-11/IP Tunnel is powered by a 24 or 48-volt station battery. It takes up 1U of space in a 19-inch rack.

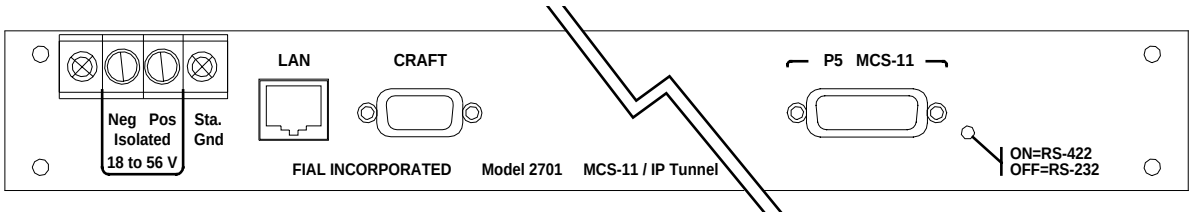


Figure 20. Rear Panel With LAN, Craft and MCS-11 Ports

Server Installation

Step 1: Install the Server in a 19-inch rack, and attach station battery, IP cable and an MCS-11 cable.

Step 2: Verify that you can locally ping Server at the address assigned to it and receive replies. This confirms the IP address setting. Also verify that the device replies to pings from another site in your network. This verifies that gateway IP address and netmask are correct.

Step 3: Connect MCS-11 Port 5 (right-most connector on rear panel) to an MCS-11 polling engine, or to a bridge or other device that provides MCS-11 polls. If polling is occurring, you should see the MCS-11 RX LED blink. If it does not blink for each poll, hold down the front panel lamp-test button for over one second. The RX and TX LEDs should blink after one second of activating the lamp-test button, indicating MCS-11 RX and TX clocks are present. If blinking does not occur, check the wiring and the DCE versus DTE settings.

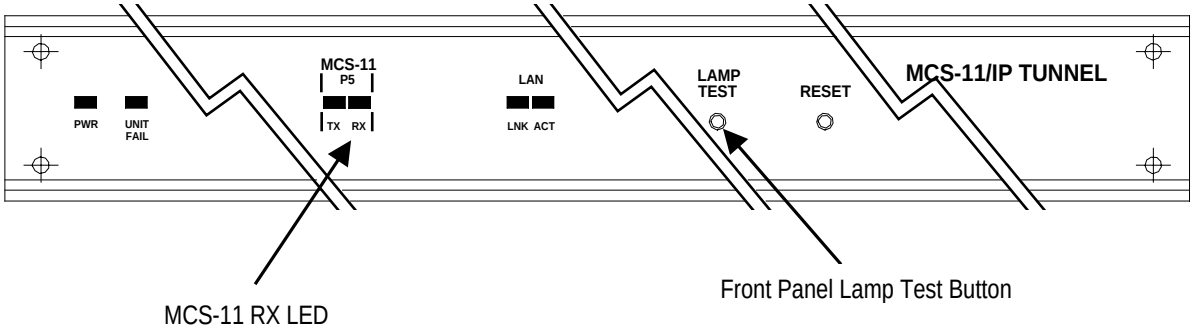


Figure 21. Front Panel

Client Installation

Step 1: Install the Client in a 19-inch rack, and attach the station battery, IP cable and an MCS-11 cable.

Step 2: Verify that the Client can be pinged at the address assigned to it. This confirms the device IP address and netmask. Also verify that the device replies to pings from another site in your network. This verifies gateway IP address and netmask as well.

Step 3: Connect the MCS-11 port or ports on the rear panel to the MCS-11 equipment that you wish to poll. Since Ports 1, 2, 3 and 4 must be supplied with a clock, connect them to DTE equipment only. Port 5 can be switched between DTE and DCE, which supplies a clock. (DTE is the most common connection used, typically to connect to microwave radios).

To switch between DTE and DCE:

A. Remove the top cover holding screw and slide out the top panel. Move the DTE/DCE slide switch to the desired position.

B. Hold the lamp test button down for longer than one second. After one second, the MCS-11 TX and RX LEDs blink if the TX and RX clock is present at the respective ports. If the LEDs do not blink, the port does not have proper MCS-11 connections.

CROSSOVER CABLE REQUIREMENTS

In an Ethernet crossover cable, pins 1 & 2 at one end are connected to pins 3 & 6 at the other end. In a normal cable (one that connects a computer to the wall or to a hub/switch), pins 1 & 2 at one end are connected to pins 1 & 2 at the other end. Also, pins 3 & 6 at one end are connected to pins 3 & 6 at the other end.

If you do not have a crossover cable, the gateway may be plugged into a hub or switch with a normal cable. Your laptop or computer must be plugged into the hub or switch with another normal cable. Then run the web browser and try again. Many new switches automatically sense the type of connection, and automatically correct for regular versus crossover connections.

NOTES

DTE versus DCE MCS-11 operation

RS-232 operation (DTE only) is mainly used to connect the MCS-11/IP Tunnel to synchronous modems. For RS-232, cable lengths must be kept short. Use 50 feet or less for 9600 baud, 25 feet or less for 19200 baud, 12 feet or less for 38400 baud. Modems should be well grounded (to rack ground) to avoid common mode noise errors. Do not try to run 56000 or 64000 baud MCS-11 with RS-232, it will not work.

MCS-11 Port 5 (the only port on the Model 2701) can be switched from the factory default DTE (accepts clock) to DCE (supplies 64 kHz clock). An internal slide-switch must be thrown to select between DCE and DTE. DTE is the most common connection used, typically to connect to microwave radios. The MCS-11/IP Tunnel cover must be removed, and the switch position changed for DCE operation. This setting is generally used when the device is configured as a Server that is directly connected to an MCS-11 polling engine. DCE is also used when the device is a Server or Client connected to a DTE port of an MCS-11 bridge.

NOTE: DCE operation only works for RS-422 – **you cannot use DCE with RS-232**. When DCE operation is selected, you can choose between normal clock (factory default) and "return clock" by moving an internal jumper. Return clock is very seldom used. Return clock is needed when the RS-422 DTE device is farther away than about 300 Meters (1000 feet), such that transmit data is so delayed that it is not properly aligned with the DCE transmit clock. All MCS-11 DTE ports return a buffered transmit clock (return clock) that is time-aligned with their transmit data.

Gateway Values

If you enter an incorrect gateway value (and then Save and Reboot), you may lose remote access through web or telnet, and the remote device may be cut off from any IP contact. A trip to the physical site of the device will be required, unless remote access to the Craft port is available.

The Craft interface can be used to correct the IP address, netmask or gateway setting. The Craft interface parameters are: 9600-baud 8N1. Each telecommunications site generally has a specific range of IP addresses available, along with a netmask and gateway (router) IP address suitable for that site. You may need to get that information from your network administrator.

Hostname

The Hostname entry on the IP_Settings screen is for operator convenience only. It allows tracking of sites by name instead of cryptic IP address. The hostname is not used for name resolution (that is, converting hostname to an IP address). Nevertheless, the hostname must be a valid Internet hostname, for example:

Only a to z, A to A, 0 to 9 and hyphen are allowed.

Underscore is no longer allowed. Case is ignored.

Valid: 65west-lake-95 (host name can start with numbers)

Invalid: west_lake (underscore not allowed anymore)

Invalid: west.lake (dot not allowed in host name)

Invalid: west-lake#95 (pound-sign not allowed)

IP Addresses

Certain IP addresses cannot or should not be used. These are the first and last addresses in the range defined by the netmask. Netmasks are used to divide the 4 billion possible IP addresses into smaller groups or "zones."

For example: Given a netmask of 255.255.255.0, IP address n.n.n.0 and n.n.n.255 cannot be used. The first is the network address, and the last is the network broadcast address. Commonly used netmasks, Class-C and smaller, are shown in the following table.

Table 1. Table of Netmasks and Addresses

Netmask	Number of Useable Addresses	Addresses That Are Not Useable
255.255.255.0	254	n.n.n.0 n.n.n.255
255.255.255.128	126	n.n.n.0 n.n.n.127 n.n.n.128 n.n.n.255
255.255.255.192	62	n.n.n.0 n.n.n.63 n.n.n.64 n.n.n.127 n.n.n.128 n.n.n.191 n.n.n.192 n.n.n.255
255.255.255.224* *see example below	30	n.n.n.0 n.n.n.31 n.n.n.32 n.n.n.63 n.n.n.64 n.n.n.95 n.n.n.96 n.n.n.127 n.n.n.128 n.n.n.159 n.n.n.160 n.n.n.191 n.n.n.192 n.n.n.223 n.n.n.224 n.n.n.255
255.255.255.240	14	n.n.n.0 n.n.n.15 n.n.n.16 n.n.n.31 n.n.n.32 n.n.n.47 etc.
255.255.255.248	6	n.n.n.0 n.n.n.7 n.n.n.8 n.n.n.15 n.n.n.16 n.n.n.23 etc.
255.255.255.252	2	n.n.n.0 n.n.n.3 n.n.n.4 n.n.n.7 n.n.n.8 n.n.n.11 etc.

For example: If the IP address zone is 192.168.0.64, and the netmask is 255.255.255.224, then 32 addresses exist in the zone, from 192.168.0.64 to 192.168.0.95. However, the address ending in 64 cannot be used, since it is the network address. Also, the address ending in 95 cannot be used since it is the broadcast address for the zone. So, only the 30 addresses from 192.168.0.65 to 192.168.0.94 may be used. Most networks use either the first or the last IP address in a zone (.64 or .94 in this example) for the gateway (router). If the destination IP address of an IP packet is not

in a device's IP address zone, then the packet is sent to the gateway. The gateway (router) 'knows' how to reach the other addresses on the LAN or Internet.

IP Port Number

The IP Tunnel must have the Server and its Clients set to the same IP port number. The Server sends packets to the client using the User Datagram Protocol (UDP) port number you set in the Server. The Clients send packets to the Server using the port number you set in the Clients. The two settings must agree. If the Server is 33333 and the Client is 40000, the Client will send packets to Server port 40000, but the Server is only listening on 33333. Likewise, The Server will send packets to Client port 33333, but the Client is only listening on 40000. Nothing will work.

If you have multiple MCS-11/IP Tunnel Servers, each with its own set of Clients, you could use the same port number for all Servers and Clients. However, it is better to use a different port number for each Server/Client(s) combination; it is easier to track down network problems using a network sniffer or packet filter.

The factory default is port 33333 and may be used in most situations. If the IP tunnel traffic must pass through firewalls, your network administrators may have to tell you what port number is open for you to use. The network administrator may need to change the firewall rules to allow UDP/IP packets with the chosen port number to pass through. Ask your network administrator to make sure that the chosen port stays open in the future!

At a minimum, the chosen port number (such as 33333) must be open for outgoing and arriving UDP/IP traffic.

If you wish to remotely provision the IP Tunnel with a web browser and view performance data, port 80 must be open in the direction of the remote IP Tunnel device for TCP/IP traffic.

If you wish to remotely provision the IP Tunnel with a telnet login, port 23 must be open for TCP/IP traffic.

Login & Password

If you forget the new Login and Password or are unable to login to the device, the Login and Password can be reset to the factory default (admin/tunnel) by holding down the lamp test button while the device is rebooted. A Login (**admin**) and Password (**tunnel**) is present in each gateway shipped from the factory. Remember that **both the login and password are case sensitive**. The login and password will allow you to have access to the Craft port or telnet and web page configuration screens. For security purposes, it is recommended that you change the login and password of each device.

If you forget the new login and password, the login and password can be reset to the factory default by holding down the lamp test button for about 15 seconds while the device is rebooted (see note 5).

If the Login/Password window will not accept your entries, it is possible that someone has changed the user name and password. Enter the correct user name and password, or see the directions

above for restoring the factory default values. NOTE: Both User Name and the Password are case sensitive.

RS 232 and RS 422

Set RS-422 **or** RS-232 operation for each MCS-11 port. If you have a single port device, that single port is port number five, not port number one. If port five will be operated in DCE (supplying clock) instead of DTE mode, change the internal switch to the DCE position. Most RS-422 input/output pins trade positions when you change this switch.

RS-232 operation (DTE only) is mainly used to connect to synchronous modems. For RS-232, cable lengths must be kept short. Use 50 feet or less for 9600 baud, 25 feet or less for 19200 baud, 12 feet or less for 38400 baud. The modem should be well grounded to rack ground to avoid common mode noise errors. Likewise, the IP Tunnel device should be well grounded to the rack ground.

NOTE: DCE operation only works for RS-422. You cannot use DCE with RS-232. When DCE operation is selected, you can choose between normal clock (factory default) and “return clock” by moving an internal jumper. Return clock is very seldom used. Return clock is needed when the RS-422 DTE device is farther away than about 300 Meters (1000 feet at 64k clock), such that transmit data is so delayed that it is not properly aligned with the DCE transmit clock.

Save & Reboot

For detailed information on Save & Reboot versus Submit, refer to the section Save & Reboot on page 19.

Web & UNIX Compatible Programs

The web configuration pages use JavaScript and Cascading Style Sheets. Microsoft Internet Explorer (IE) version 5.0 or later is recommended. Netscape 7.0 installed for Windows 2000 has been tested and also works well.

When Netscape is used on UNIX machines, you must turn on JavaScript and Cascading Style Sheets. These are often turned off by default on earlier versions of Netscape for Unix/Linux. Use UNIX Netscape version 7.0 or later. Netscape 4.7 does *not* work with the IP address drop-down boxes.