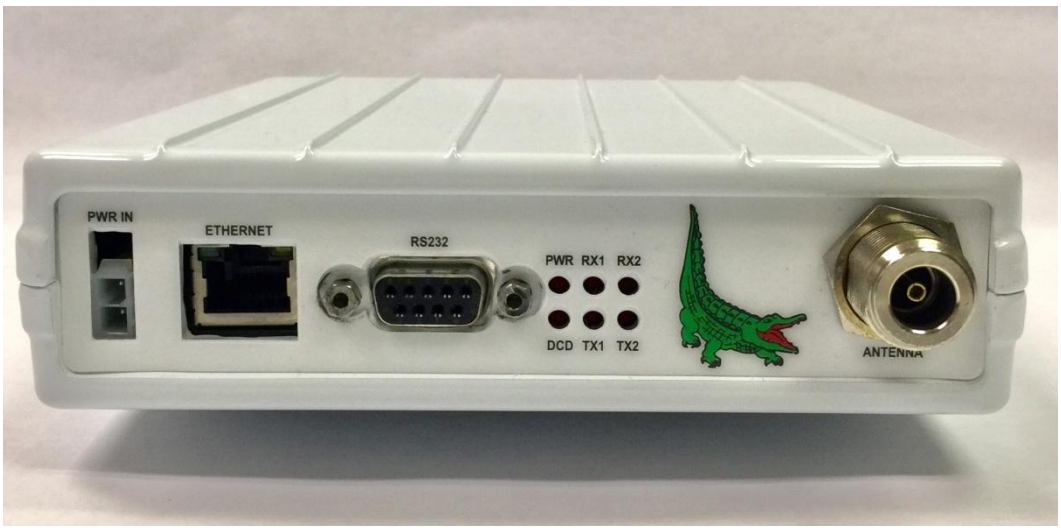
Model 2788 MAS Ethernet/RS-232 UHF Radio Transceiver Technical Manual



Alligator
Communications, Inc

REVISION HISTORY

REV	DESCRIPTION	DATE
1	Initial Release	10/15/2018

Paragraph *Contents* *Page*

1. 5

1.1 General Description5

1.2 Applications5

1.3 Technical Specifications6

1.4 Warranty8

1.5 Claims for damage in shipment8

1.6 Information to user, as required by FCC section 15.219

1.7 RF exposure information9

2.0 Radio Configuration and Operational Check10

2.1 General Discussion10

2.2 Operational Bench Test10

2.2.1 Antenna Connector10

2.2.2 Power Connector11

2.2.3 Initial Checkout11

3.0 Field Configuration and Verification15

3.1 15

4.0 Front Panel Indicators17

5.0 User Configuration and Diagnostic Menu18

5.1 18

5.2 18

5.3 18

5.4 19

5.5 19

5.6 19

5.7 19

5.8 19

5.9 20

5.10 Subnet Mask20

5.11 RS-232 Data Rate20

5.12 Anti-streaming Timer20

5.13 Telnet Session Activity Timer20

5.14 Log-in Session Activity Timer20
5.15 Enable Transmitter21
5.16 Enable Encryption21
5.17 Enable Password Entry21
5.18 ID (Identification Number)21
5.19 Password21
5.20 ES Encryption Phrase21
5.21 Log Out22
5.22 Quit Telnet22
5.23 Forwarding Mode22
5.24 Remote RTU0 MAC Address22
5.25 Remote RTU1 MAC Address23
5.26 Master RTU MAC Address Table23
5.27 Host MAC Address Table23
5.28 High QOS (Quality Of Service) IP Address Table23
5.29 Loopback Remote MAC Address24
5.30 Diagnostic Tests24
5.31 Display Status Screen25
5.32 Display RTU Table25
5.33 Display Host Table25
5.34 Display QIP Table25
6.0 Theory of Operation26
6.1 RS-232 Communications26
6.2 Ethernet Communications26
6.2.1 Packet Forwarding26
6.2.2 Telnet Radio Configuration and Diagnostics27
6.2.3 Graphics Heavy Communications27
6.2.4 High QOS (Quality Of Service) IP Communications27

Introduction

Thank you for purchasing the Alligator Model 2788 UHF Radio Transceiver. We are here to assist you personally should any questions arise in the installation or operation of this product. Please feel free to call us. We look forward to your feedback and will strive to make our product as compliant with your specific needs as possible.

1.1 General Description

The Alligator Communications Model 2788 is a microprocessor-controlled data radio transceiver designed to operate in accordance with FCC rules, Parts 27 and 90 The 2788 data radio is frequency synthesized and programmable to individual transmitter and receiver frequencies in the 757 and 788 MHz frequency band. The transceiver is a fixed channel, half-duplex radio available with a channel bandwidth of 12.5 kHz and up to 100 kHz. It interfaces with both Ethernet and RS-232.

1.2 Applications

The 2788 data radio is designed for point-to-multipoint or point-to-point licensed operations in the 700 MHz band. Some of the most common applications are:

- Electric Utility Substation SCADA
- Pipeline Flow Monitors
- Energy Distribution & Metering Applications
- Gas or Petroleum Production Well Head Control and Monitoring
- Water Distribution and Waste Water Collection Control and Monitoring
- Petroleum Production, Transmission, Storage and Distribution
- Railroad

1.3 Technical Specifications

GENERAL	
Frequency	787-788 MHz
Input Voltage	10-24 Vdc
Current Consumption (at 13.8 Vdc)	<80 mA
Receive Mode	100 mA
Transmit Mode (0.2 Watts)	< 0.5 A
Data Rate	9600 bps to 38.4 kbps
Connectors	
Antenna	Type N female
Power	2-pin Captive, Rectangular
Data (RS-232)	DB9F
Environment	
Temperature	-30°C to +50°C
Humidity	95% at 40°C
Dimensions	6.75” x 1.5” x 5.75”
Weight	2 pounds

TRANSMITTER

RF Power	2 W
Impedance	50 Ohms
Frequency Range	757-758 MHz
Frequency Step Size	1 Hz
Frequency Stability	±1 ppm
Modulation	4GFSK
Symbol Rate	4800 Hz**
Data Rate	9600 bps
Maximum Frequency Deviation	2400 Hz**
Attack Time	<1 msec
Release Time	<0.5 msec
Bandwidth	6.25, 12.5, 25, or 50 kHz**

RECEIVER

Input Sensitivity	-117 dBm at 10^{-6} BER
Impedance	50 Ohms
Frequency Range	757-758 MHz
Frequency Step Size	1 Hz
Frequency Stability	±1 ppm
Selectivity	100 dB
Desensitization	-60 dB
Intermodulation	-75 dB (EIA)
Spurious Image Rejection	-80 dB
Bandwidth	6.25, 12.5, 25, or 50 kHz**

deviation

1.4 Warranty

Alligator Communications, Inc., warrants each of the instruments of its manufacture to meet the specifications when delivered to the BUYER; and to be free from defects in material and workmanship. Alligator Communications will repair or replace, at its expense, for a period of one year from the date of delivery of equipment, any parts that are defective from faulty material or poor workmanship. This Warranty does not cover equipment which has been misused and/or altered by the user.

Instruments found to be defective during the warranty period shall be returned to the factory with transportation charges prepaid by the BUYER. It is expressly agreed that replacement and repair shall be the sole remedy of the SELLER with respect to any defective equipment and parts hereof and shall be in lieu of any other remedy available by applicable law. All returns to the factory must be authorized by the SELLER, prior to such returns. Upon examination by the factory, if any instrument is found to be defective, the unit will be repaired and returned to the BUYER, with transportation charges prepaid by the SELLER. This warranty does not apply to equipment which, in the opinion of the SELLER, has been altered or misused.

NO OTHER WARRANTY IS EXPRESSED OR IMPLIED. ALLIGATOR COMMUNICATIONS IS NOT LIABLE FOR CONSEQUENTIAL DAMAGES.

1.5 Claims for damage in shipment

The instrument should be inspected and tested as soon as it is received. If the instrument is damaged in any way, or fails to operate properly, a claim should immediately be filed with the freight carrier, or, if insured separately, with the insurance company.

WE PLEDGE OUR IMMEDIATE AND FULLEST COOPERATION TO ALL USERS OF OUR ELECTRONIC EQUIPMENT.

PLEASE ADVISE US IF WE CAN ASSIST IN ANY MANNER:

Alligator Communications, Inc.

1400 Coleman Avenus

Santa Clara, CA 95050

Phone: (408) 327-0800

FAX: (408) 327-0808

E-mail: info@alligatorcom.com

Website: www.alligatorcom.com

1.6 Information to user, as required by FCC section 15.21

Changes or modifications not expressly approved in writing by Alligator Communications, Inc. may void the user's authority to operate this equipment.

In accordance with FCC Rules Section 15.21, the user of this equipment is advised that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

1.7 RF exposure information

FCC Rule Section §1.11307 and Industry Canada RSS-102 regulations contain limits on human RF exposure from transmitters. To meet these requirements, during operation, the antenna of this device must be kept at a minimum distance of 112 cm from all persons.

2.0 Radio Configuration and Operational Check

2.1 General Discussion

Prior to customer installation and electrical connection of the customer's terminal equipment to the 2788 radio, it is recommended that the installing technician conduct a brief operational checkout of the 2788 radio and confirm that all operating parameters are set as desired.

This initial checkout and possible reprogramming/customization is generally performed on the maintenance shop test bench before the radio is installed and commissioned in a link application.

The following parts of this section provide guidance in this checkout process and illustrate alternate configurations and paths to perform the initial checkout.

2.2 Operational Bench Test

To ensure that the 2788 radio is functional prior to installation at the desired site, it is highly recommended that the following tests be performed in sequence: (Please refer to 2.2.3 Initial Checkout.)

2.2.1 Antenna Connector

The 2788 radio antenna port (RF Connector) is a coaxial, female, Type N connector. This connector mates with a male cable connector, Type N such as Amphenol 3900, Andrew L44N, or MIL Type UG-21. Under most circumstances, bench tests are conducted with a service monitor (manufactured by IFR Inc., Marconi Instruments Ltd., Hewlett-Packard, Motorola, etc.).

CAUTION
The transmitter should not be keyed on or placed in the transmit mode without a load connected to the antenna port to prevent damage to the 2788 radio Power Amplifier due to long periods (more than 10 minutes) of severely high SWR. An antenna, service monitor, or dummy load should be attached to the antenna port. The 2788 radio power output is approximately 2 Watts maximum, so if a service monitor is connected to the antenna port, ensure that the service monitor's input port can handle at least a 5 watt input to avoid damaging the service monitor.

2.2.2 Power Connector

The DC power input connector to the 2788 radio is a rectangular two-pin locking connector. The radio unit is normally powered upon connection to a DC power source of +11 to +24 Vdc, +13.8 Vdc (nominal). The red conductor is positive; the black conductor is negative and is internally grounded to the chassis.

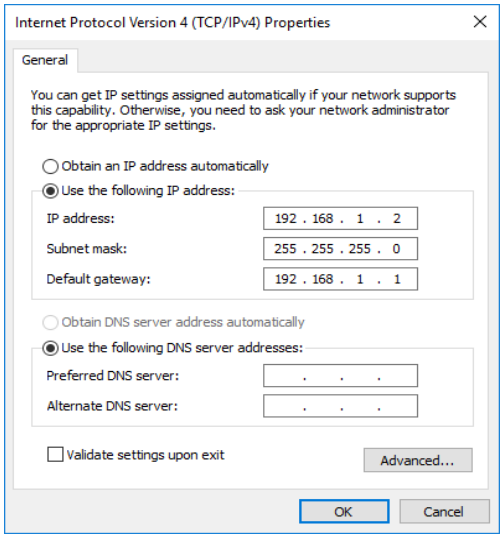
2.2.3 Initial Checkout

Alligator wireless data transport products are factory-configured according to customer configuration information received prior to shipment from the factory; thereby, customer field configuration requirements are minimized.

To verify that 2788 radio parameters are correct, we recommend the following minimal tests be conducted with regards to the transmitter and receiver settings of the 2788 radio:

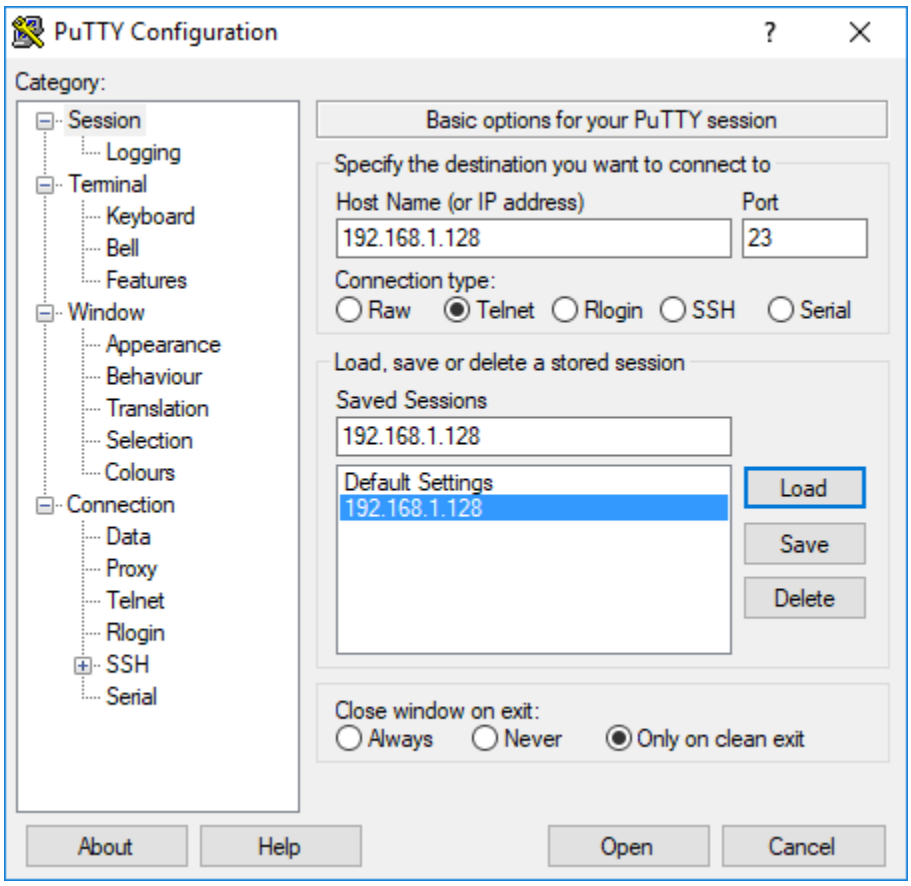
1. Connect a 50 Ohm dummy load to the antenna Type N connector. The dummy load must have a power rating of at least 5 Watts. Always insure that a load or antenna is connected to the Type N connector before DC power is applied.
2. Connect a spectrum analyzer to the dummy load through a power attenuator (30 dB recommended).
3. Connect a computer to the 2788 using a CAT5 Ethernet cable between Ethernet connectors. Alternatively, you may use two CAT5 cables, each connected to a multiport Ethernet router switch. Do not use an Ethernet hub because they may be a source of errors.
4. Connect a 12Vdc power source to the power input, +12V on red, GND on black. Observe all LEDs activate at power-up to verify LED functionality. The PWR LED should remain on.

5. Configure your computer for an IP address in the 192.168.1.X space (but do not use 192.168.1.1 or 192.168.1.128). This can be changed later, but is necessary for initial Telnet communication with the 2788. For example, use 192.168.1.2 .

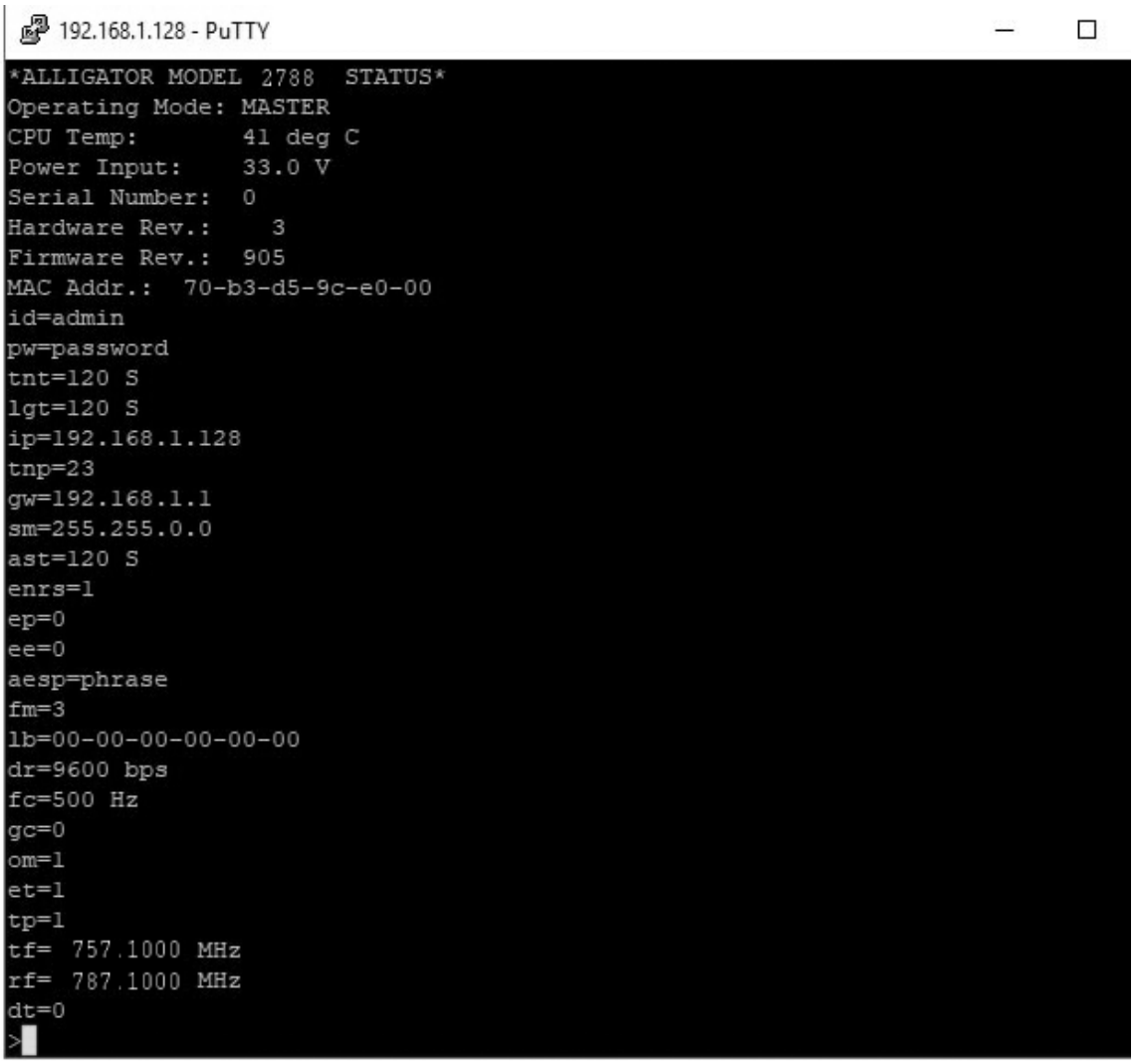


6. Download a Telnet client program for use on your lap-top such as puTTY. Configure puTTY to communicate to the 2788 on its IP address. The normal default IP address and port for the 2788 is 192.168.1.128 port 23.

Below shows a typical puTTY configuration for communicating with the 2788 on IP default address 192.168.1.128 port 23. Be sure to have your computer IP address set in the subnet range. puTTY should have Terminal set for local echo on. For example, below the computer has an IP address of 192.168.1.2 and communicates via Telnet to the 2788 on the default IP address 192.168.1.128 port 23.



7. Open a Telnet session with the 2788. You should get a menu showing the current 2788 status and configuration (Fig. 2). You may end a Telnet session at any time by entering q. The menu can be re-displayed by either entering <CR> or <ESCAPE>.



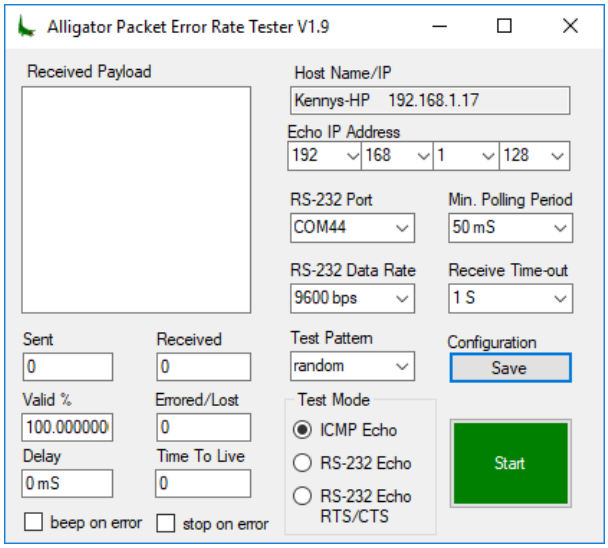
8. Set the desired transmitter frequency. For example, tf=757.0950.0<CR>.
9. Set the desired receiver frequency. For example, rf=787.0940.0<CR>.
10. Set the desired transmit power. For example, tp=1<CR>.
11. Use the dt=1<CR> command to activate the transmitter carrier in CW mode to confirm frequency and RF level on a spectrum analyzer. You will have 120 seconds before the anti-streaming timer expires and deactivates the CW carrier. Typing <ESCAPE> or <ENTER> will deactivate the CW carrier.
12. You may run other optional tests to verify radio functionality:

a. Connect two 2788 radios together using suitable attenuators and coaxial cable. Configure one radio to transmit CW (dt=1<CR>) and the other to receive CW (dt=2<CR>). The receiver displays the received signal strength in dBm.

b. Connect two 2788 radios together using suitable attenuators and coaxial cable. Configure one radio to be a master (om=1<CR>) to send test packets (dt=3) and the other to be a remote (om=0) to receive test packets (dt=4<CR>. The receiver will monitor the number of good and bad test packets received in this one-way test.

c. Connect two 2788 radios together using suitable attenuators and coaxial cable. Configure one radio to be a master (om=1<CR>) to send a round-trip test packet (dt=5) to the remote radio. The master 2788 radio must also be given the 2788 MAC address of the remote radio. To enter the remote loop-back MAC address, enter:
lb=##-##-##-##-##-##
The remote radio (om=0<CR> will automatically echo back packets when in the dt=0<CR> configuration.

13. Alligator provides software testing tools to do end-to-end testing such as the Alligator Packet Error Rate Tester. For example, Alligator provides software tools for simulating a host sending random data messages to keep track of errors that are not echoed back properly by an RTU simulator tool.



3.0 Field Configuration and Verification

Prior to field installation of the 2788, it is crucial that that bench configuration and testing be done using cables and RF attenuators to duplicate the deployed system or subsystem. This adds confidence that the configuration has been done properly and stream-lines field installation.

Each remote configured 2788 must be tested with a master configured 2788 to verify proper operation. This places deployed radios in final configuration so no additional programming is necessary when final field installation is performed. This is highly recommended for a smooth system deployment.

3.1 Field Configuration Bench Test

1. Update the 2788 IP address to the desired fielded IP address. Each 2788 must be assigned to a unique IP address in the subnet of the access point router. For example, ip=10.0.0.5<CR>. Once this instruction is entered, the Telnet connection is lost and must be re-established on the new IP address.
2. Re-establish Telnet communications on the new IP address. Typically use a second lap-top with its IP address configured to the desired IP subnet range and with a copy of puTTY that can start a Telnet session with the 2788 on the newly assigned IP address.
3. Assign the access point router gateway IP address. For example, gw=10.0.0.1<CR>.
4. Assign the subnet mask. For example, sm=255.255.255.0 .
5. If desired, assign a different Telnet port from the default port 23. For example, tnp=50000<CR>. If you change the Telnet port, you lose the session and must reconnect on the newly assigned port number with puTTY.
6. Assign a group code if desired to identify a unique group of radios. This blocks accidental communications with other 2788 radios. For example, gc=3<CR>.
7. Decide if the 2788 is a master or remote. There is only one master 2788 radio in a point-to-point or point-to-multipoint radio network. For a master, configure with the command om=1<CR>. For a remote, configure with the command om=0<CR>. The primary difference between a master and remote is that a master passes host polls and other unsolicited messages. The remote radio passes responses from the polled RTU. Occasionally the RTU generates unsolicited transmissions to the remote radio. This causes no disturbance to the polling process. The remote radio buffers the packet(s) until a clear time to send back to the host. Note that both the master radio and remote radios are transparent to the protocols encapsulated in the Ethernet packets or RS-232 serial data.
8. If using RS-232, select the terminal data rate. The data rate can be selected from 1200, 2400, 4800, 9600, or 19200 bps. For example, dr=9600<CR> selects 9600 bps. Note that in RS-232 systems, the Ethernet connector is still used for Telnet control of the 2788. The 2788 can handle RS-232 and Ethernet concurrently.
9. The 2788 has various forwarding modes to limit Ethernet access to the radio network at both the master and remotes ends of the radio link. This aids in preventing flooding the radio network with unwanted packets. The 2788 shipping default is fm=3<CR>. This

mode forwards all packets (known as promiscuous packet forwarding mode). This mode is only recommended for small systems and testing. The recommended mode is fm=1<CR> (host mode forwarding). In this mode a master radio will only forward packets with a tabulated host source MAC address. A remote radio in host forwarding mode only forwards packets with a tabulated host destination MAC address. Up to 16 addresses can be stored in the 2788 remote or master radio. For additional flooding protection, additional filtering can be configured to perform RTU MAC filtering also. The host 2788 radio can maintain a table of up to 512 RTU MAC addresses. Each remote 2788 radio can maintain a table of up to 2 RTU MAC addresses. Refer to the command summary for entering and reading RTU and host MAC addresses.

10. When using host forwarding (fm=0 or fm=1) on either the master or remote 2788 radio, determine the host MAC Ethernet address and enter it in the host table using the command: host[n]=##-##-##-##-##-##<CR>, where n is a lower case hexadecimal number 0,1,2,3,4,5,6,7,8,9,a,b,c,d,e, or f.

    Up to 16 host MAC addresses may be stored in the host table memory. Each MAC address contains 6 bytes, in lower case hexadecimal, with hyphen separators between individual bytes. Enter hosttable<CR> to display the host table.
11. When using master RTU forwarding (fm=0 or fm=2), the master 2788 radio (om=1) must contain a list of all RTU MAC addresses (up to 512). Enter an RTU address using the following command: rtu[abc]=##-##-##-##-##-##<CR>, where abc is a lower case hexadecimal number from 000 to 1ff (0 to 511 decimal). Enter rtutable<CR> to display the RTU table on a 2788 radio configured as a master (om=1).
12. When using remote RTU forwarding (fm=0 or fm=2), the remote 2788 radio (om=0) contains a list of up to 2 RTU MAC addresses. These addresses correspond to the RTUs connected to that particular remote 2788 radio. The first RTU MAC is entered with the following command: rtu0=##-##-##-##-##-##<CR>. The second (if any) RTU MAC address is entered with the following command: rtu1=##-##-##-##-##-##<CR>. These two MAC addresses are displayed in the regular status menu on a 2788 radio configured as a remote (om=0).
13. Access to the 2788 can be restricted to personnel knowing an id and password. To enable this password protection, enter the following command: ep=1<CR>. The id is set using: id=### . . . ###<CR>, where the id is up to 16 characters and is case sensitive. The password is set using: pw=### . . . ###<CR>, where the password is up to 16 characters and is case sensitive. The default id is *admin* and the default password is *password*. Once a session is completed, the user logs out using the log out command: lo<CR>.

    Should the user forget to log out, it will automatically log out due to user keyboard inactivity after the lgt time. Should the password and/or id be forgotten, the factory default can be restored by removing the 2788 cover and pressing the push button. (See Fig. 3) The push button also restores the original defaults for the IP address, subnet mask, and gateway. To disable password protection, either press the push button or enter ep=0<CR>.

14. The 2788 can operate using the AES256 encryption standard with the following commands:
    ee=0<CR> no encryption
    ee=1<CR> AES256 encryption

    No encryption results in the least number of extra characters appended to a message. This minimizes transmission latency. Encryption will pad extra randomized characters to create standardized message segment lengths of 128 bits. The pad characters are removed at the receiver.

    The AES256 standard uses a 256-bit key. The key is generated from a user generated phrase. This phrase can be up to 32 case sensitive characters. It is entered with the command: aesp=### . . . ###<CR>. The phrase is converted into a 256 bit key using the SHA256 secure hashing algorithm. This key is used by the AES256 encryption and decryption algorithms.
15. Should it be necessary, the transmitter can be disabled with the command: et=0<CR>. To re-enable the transmitter: et=1<CR>.

4.0 Front Panel Indicators

The six front panel LEDS are defined in Table 1:

LED	Description
PWR	On when 12 Vdc power is applied.
RXD1	On when receive data is active.
RXD2	On when diagnostic receive data is active.
DCD	On when receive data preamble is detected.
TXD1	On when transmit data is active.
TXD2	On when diagnostic transmit data is active.

Table 1 LED Definition

The LEDs show the status of both Ethernet and RS-232 serial data. Diagnostic data occurs during Telnet sessions.

5.0 User Configuration and Diagnostic Menu

The 2788 uses a simple command line interface for configuring and monitoring key parameters and metrics. Access is via IP Telnet. The 2788 is set to a default IP address of 192.168.1.128 at time of shipment. The access is either local, using the Ethernet RJ-45 connector or remote through the radio system. The command line interface facilitates writing scripts for automated configuration. Contact Alligator for GUI based software utilities that front-end the Telnet commands to simplify network management of multiple 2788 radios further .

Should it ever be necessary, an internal push-button resets the IP address to the default of 192.168.1.128 and default Telnet port to 23. The push-button also resets the password, encryption phrase, and takes the unit out of password mode. The remaining parameters are unchanged. (See Fig. 3)

5.1 Transmitter Frequency

The transmitter frequency is set in MHz with up to 9 significant figures. The allowed frequency range is from 757 to 788 MHz. The full format is:

tf=###.######<CR>

The decimal point is optional. Trailing zeros are optional.

Examples: 757<CR> 757.0<CR> 757.1<CR> 757.12<CR> 757123456<CR>

5.2 Receiver Frequency

The receiver frequency is set in MHz with up to 9 significant figures. The allowed frequency range is from 757 to 788 MHz. The full format is:

rf=###.######<CR>

The decimal point is optional. Trailing zeros are optional.

Examples: 757<CR> 757.0<CR> 757.1<CR> 757.12<CR> 757123456<CR>

5.3 Frequency Calibration

The 2788 frequency reference is a precision TCXO (Temperature Compensated Crystal Oscillator) that is factory tuned to 1 ppm accuracy. Should it ever be necessary to adjust the compensation, the following command permits trimming the PLL multiplier that directly affects the TX and RX frequencies in steps of 1 Hz:

fc=xxxx<CR>

Examples: 100<CR> -100<CR> 10<CR> -10<CR>

Normally calibration is performed by transmitting a CW carrier (dt=1) and monitoring the output frequency on a calibrated frequency counter.

5.4 Transmit Power

The 2788 transmitter output power has three power settings:

1 = Low (0.5 W); 2 = Mid (1 W) ; 3 = Hi (2 W)

tp=x<CR>

Examples: tp=1<CR> ; tp=2<CR> ; tp=3<CR>

5.5 Operational Mode

The 2788 has two operational modes:

0 Remote
1 Master

Systems can be configured for single or dual frequency. No advantage in latency is gained by using two channel frequencies.

Systems use 1 master (om=1) and up to 512 remotes (om=0). It requires that the master have line of sight to all remote radios.

om=x<CR>

Examples: om=0<CR> ; om=1<CR>

5.6 Group Code

To prevent confusion of two or more separate 2788 systems, there are 16 unique group codes to distinguish 2788 groups, ranging from 0 to 15. The default group code is 0.

gc=##<CR>

Examples: gc=0<CR> ; gc=1<CR>; gc=15<CR>

5.7 IP Address

Each 2788 radio must be assigned a unique IP address within its LAN subnet group. This permits both local and remote access of radio configuration and status information. The default IP address is 192.168.1.128. It must be changed prior to field deployment. The IP address assigned to the radio is for diagnostic purposes to control and monitor the 2788 locally or remotely.

ip=###.###.###.###<CR>

Examples: ip=10.0.0.100<CR> ; ip=172.16.10.100; ip=192.168.1.10<CR>

If the IP address is changed to a new subnet, make certain that the computer is also changed to the new subnet.5.8 Telnet Port

The 2788 Telnet port can be reassigned from the default of 23 to any port up to 65535. This adds additional security to the system.

tnp=#####<CR>

Examples: tnp=23<CR>; tnp=1000<CR> ; tnp=65535<CR>

5.9 Gateway Address

The 2788 must be given the gateway router IP address within its LAN subnet group. Normally it is the first IP subnet address ending in 1.

gw=###.###.###.###<CR>

Examples: gw=10.0.0.1<CR>; gw=172.16.10.1; gw=192.168.1.1<CR>

5.10 Subnet Mask

The 2788 must be given a subnet mask. The default is 255.255.0.0

sm=###.###.###.###<CR>

Examples: sm=255.255.0.0<CR> ; sm=255.255.255.0

5.11 RS-232 Data Rate

The 2788 has a DB9 connector to permit using an RS-232 interface. The asynchronous data format is one start bit, eight data bits, and one stop bit with no parity. The data rate can be set to one of five possible rates: 1200 bps, 2400 bps, 4800 bps, 9600 bps (default), and 19200 bps.

dr=####<CR>

Examples: dr=1200<CR> ; dr=2400<CR> ; dr=4800<CR> ; dr=9600<CR> ; dr=19200<CR>

5.12 Anti-streaming Timer

The transmitter key on time is timed to prevent disrupting the channel. The maximum on time is the anti-streaming time defined in seconds. The default is 120 seconds. This is most often invoked when performing testing with a CW carrier that is activated remotely.

ast=####<CR>

Examples: ast=120<CR>; ast=9999<CR>

5.13 Telnet Session Activity Timer

The 2788 times activity when engaged in Telnet communications. If there is inactivity for more than the specified time duration in seconds, the Telnet session is automatically terminated. The default Telnet session activity timer default is 120 seconds.

tnt=####<CR>

Examples: tnt=300<CR> ; tnt=9999<CR>

5.14 Log-in Session Activity Timer

The 2788 times activity when using password access (pw=1). If there is inactivity for more than the specified time duration in seconds, the log-in session is automatically terminated. The default log-in session activity timer default is 120 seconds.

lgt=####<CR>

Examples: lgt=300<CR>; lgt=9999<CR>

5.15 Enable Transmitter

The 2788 transmitter can be enabled for normal operation or forced to be disabled by this command.

et=#<CR> 0 = disable transmitter 1 = enable normal transmitter operation

Examples: et=0<CR> ; et=1<CR>

5.16 Enable Encryption

The 2788 can encrypt data for additional data security. This command selects encryption.

ee=#<CR> 0 = disable encryption 1 = enable AES256 encryption

Examples: ee=0<CR> ; ee=1<CR>

5.17 Enable Password Entry

The 2788 can restrict access by forcing an id and password before access is granted.

ep=#<CR> 0 = disable password entry 1 = enable password entry

Examples: ep=0<CR> ; ep=1<CR>

5.18 ID (Identification Number)

When password entry is enabled (ep=1), this ID must match to gain access to the 2788. The ID is case sensitive and can be any set of up to 16 characters, including letters, numbers, and punctuation marks. The default id is “admin”.

id=###. . .###<CR>

Examples: id=<CR> ; id=admin<CR>

5.19 Password

When password entry is enabled (ep=1), this password must match to gain access to the 2788. The password is case sensitive and can be any set of up to 16 characters, including letters, numbers, and punctuation marks. The default password is password.

pw=###. . .###<CR>

Examples: pw=<CR> ; id=password<CR>

5.20 ES Encryption Phrase

When encryption is enabled (ee=1), a case sensitive phrase of up to 32 characters including letters, numbers, and punctuation marks is hashed to a 256-bit AES256 encryption key using the SHA256 secure hashing algorithm. This key is used encrypt and decrypt 128- bit message fragments used in the AES256 encryption standard.

aesp=###. . .###<CR>

Examples: aesp=<CR> ; aesp=mydoghasfleas<CR>

5.21 Log Out

When password entry is enabled (ep=1) after a session is complete, the user logs out using the command:

lo<CR> (lower case L lower case O)

If the lo<CR> is not entered, then the session timer will automatically perform the log out after timing out.

5.22 Quit Telnet

To quit a Telnet session:

q<CR>

5.23 Forwarding Mode

The 2788 forwards all RS-232 transmissions; however, Ethernet packets are forwarded more selectively to avoid RF network flooding. There are four forwarding modes:

1 RTU and Host (qualified RTU and Host source/destination MAC address)
2 Host (qualified host source/destination MAC address)
3 RTU (qualified RTU source/destination MAC address)
4 All (No filtering, all packets forwarded)

fm=#<CR>

The factory default is fm=3, but it is highly recommended that it be changed to fm=1 (host forwarding) to prevent flooding. Host filtering is easily done by entering the host MAC address in the host and remote 2788 radios. At the master only host sources are forwarded. At the remote only host destinations are forwarded. Up to 16 host MAC addresses can be placed in the host MAC address table.

RTU MAC address filtering offers additional traffic flooding protection. The master radio can store up to 512 remote RTU MAC addresses. The remote radios can store up to two RTU MAC addresses associated with the RTUs connected to that remote radio.

Examples: fm=0<CR>; fm=1<CR> ; fm=2<CR>; fm=3<CR>

5.24 Remote RTU0 MAC Address

This is the RTU MAC hexadecimal address of the first RTU connected to a remote 2788. It is stored at the remote 2788 and is used when the remote radio is in forwarding mode 0 or 2.

rtu0=##-##-##-##-##-##<CR>

Example: rtu0=01-23-45-ab-cd-ef<CR>

5.25 Remote RTU1 MAC Address

This is the RTU1 MAC hexadecimal address of the second RTU connected to a remote 2788. It is stored at the remote 2788 and is used when the remote radio is in forwarding mode 0 or 2.

rtu1=##-##-##-##-##-##<CR>

Example: 01-23-de-ad-be-ef<CR>

5.26 Master RTU MAC Address Table

This is the command format for entering RTU hexadecimal addresses in the master radio RTU table. It is used when the master is in forwarding mode 0 or 2. Up to 512 RTU MAC addresses may be saved in the master RTU MAC address table. Both RTU number (000 to 1ff) and associated MAC address are in hexadecimal. The table is initially cleared to all zeros. Normally the table is filled, starting at 000 and progressing to a maximum number of 1ff. The entire table is scanned for each forwarding operation by the master radio when fm=0 or fm=2.

rtu[###]=##-##-##-##-##-##<CR>

Example: rtu[000]=01-23-45-ab-cd-ef<CR> ; rtu[1ff]=01-23-de-ad-be-ef<CR>

5.27 Host MAC Address Table

This is the command format for entering host hexadecimal addresses in the 2788 host table. It is used when either the master or remote radio is in forwarding mode 0 or 1. Up to 16 host MAC addresses may be saved in the host address table. Both host number (0 to f) and associated MAC address are in hexadecimal. The table is initially cleared to all zeros. Normally the table is filled, starting at 0 and progressing to a maximum number of f. The entire table is scanned for each forwarding operation by the master or remote radio when fm=0 or fm=1.

host[#]=##-##-##-##-##-##<CR>

Example: host[0]=01-23-45-ab-cd-ef<CR> ; host[f]=01-23-de-ad-be-ef<CR>

5.28 High QOS (Quality Of Service) IP Address Table

This is the command format for entering high QOS IP addresses in the 2788 QIP table. Most commonly the IP address of polling host computers is entered into both the master radio QIP table and all remote QIP tables. This gives priority for high QOS device sources at the master radio and high QOS destinations at the remote radios.

Up to 16 IP addresses may be saved in the QIP table. Host number (0 to f) is in hex and associated IP addresses are in standard dot notation. The table is initially cleared to all zeros. Normally the table is filled, starting at 0 and progressing to a maximum number of f.

Note that RS-232 always has high priority since it is most commonly used for polled systems.

host[#]=###.###.###.###<CR>

Example: host[0]=192.168.1.2<CR> ; host[1]=192.168.1.3<CR> ; host[f]=10.0.0.10<CR>

5.29 Loopback Remote MAC Address

This is the remote radio hexadecimal MAC address placed in the master radio when performing the loopback diagnostic test (dt=5). Note that Alligator 2788 radios are currently assigned to MAC addresses starting with 70-b3-d5-9c-e.

lb=##-##-##-##-##-##<CR>

Example: lb=70-b3-d5-9c-e0-00

5.30 Diagnostic Tests

There are several different diagnostic tests that can be performed using the dt command:

1 TX CW
2 RX CW
3 TX 1 Way
4 RX 1 Way
5 TX 2 Way
6 Display TX Buffer
7 Display RX Buffer
8 Display TX and RX Buffers
9 Display Sub-packet Types

dt=#<CR> Note that <ESC> terminates the test, returning to dt=0.

Example: dt=1<CR> dt=5<CR>

The default at power-up is 0 (none).

5.31 Display Status Screen

The status screen is displayed by two methods:

<ESC> a single press of the escape key

<CR><CR> a double press of the carriage return (ENTER key)

5.32 Display RTU Table

The entire 512-entry RTU table is displayed:

rtutable<CR>

5.33 Display Host Table

The entire 16-entry host table is displayed:

hosttable<CR>

5.34 Display QIP Table

The entire 16-entry QIP table is displayed:

qiptable<CR>

6.0 Theory of Operation

The 2788 concurrently operates transparently using two communication interfaces: Ethernet and RS-232 (Fig. 1). The 2788 encapsulates any protocol in a proprietary Alligator format to encrypt and forward multiple packet fragments across a UHF radio link and reassemble them seamlessly. It is most easily understood as a wire transmission with added latency due to time taken for transmission over a 12.5 kHz channel at 9600 bps along with delays due to packet screening, assembly and encryption.

6.1 RS-232 Communications

The RS-232 communications interface forwards all incoming serial data with no screening. It operates at one of five programmable data rates: 1200, 2400, 4800, 9600, 19200 and 38400 bps. There is no RTS or CTS data flow control required because data is forwarded based on TXD line activity. This permits a simple three wire interface consisting of TXD, RXD, and GND.

6.2 Ethernet Communications

All Ethernet packets (UDP, TCP/IP, Ping, ARP, . . .) are recognized and can be transparently forwarded over the RF network.

6.2.1 Packet Forwarding

The Ethernet communications interface forwards incoming IP packets, provided that they pass a user-programmable forwarding screening test. Packet forward screening is done to minimize data traffic not intended for the radio network that could otherwise flood the system. The 2788 has four programmable forwarding modes:

1. No Screening
2. Host Screening
3. RTU Screening
4. RTU and Host Screening

The simplest forwarding mode does not screen any packets. This is referred to as the IP promiscuous mode and is only used in small systems where flooding by unwanted packets is improbable. It is not recommended in systems with either the master or remote ends tied to LANs due to the flooding potential. The 2788 defaults in this mode for testing but is not recommended for field deployment.

The host screening mode is highly recommended for packet forwarding on the master radio. At the master radio, a host table with up to 16 entries is created by the user with a list of host MAC addresses. Only packets originating by authorized hosts on the MAC table are forwarded. The remote radio can also be configured for host filtering. This causes the remote radio to forward only packets originating from the RTU back over the RF link that are destined for an authorized host MAC address. This greatly reduces the probability of system flooding.

The RTU screening mode is used so that only packets destined for authorized RTU MAC addresses are forwarded. At the master radio, an RTU table with up to 512 entries is created by the user with a list of RTU MAC addresses. Only packets destined for authorized RTUs on the

MAC table are forwarded. The remote radio can also be configured for RTU filtering. This causes the remote radio to forward only packets back over the RF link when they are sourced by an authorized source RTU MAC address. This also greatly reduces the probability of system flooding.

The combined RTU and Host screening mode provides the greatest amount of filtering. Only authorized traffic has access to the radio address with both source and destination MAC address complying with the system definition. This makes system flooding nearly impossible to occur.

6.2.2 Telnet Radio Configuration and Diagnostics

The primary mission of the 2788 is to provide robust RF linkage with total protocol transparency; however, a Telnet server for local and remote radio configuration is provided in each 2788. Thus, each 2788 is factory-assigned a unique Alligator MAC address for IP access using the Telnet protocol. The user is able to program the IP address, gateway address, subnet mask, and Telnet port address. This gives the radio visibility to the host and/or a separate client host for radio configuration and diagnostics. Users of RS-232 interfaces also use the Ethernet interface with a Telnet client program. The Telnet communications over the RF link shares the bandwidth of the system transparently.

6.2.3 Graphics Heavy Communications

The use of communications carrying a large amount of graphics data is discouraged. Please be aware that at 9600 bps, the transmission rate is only about 1K bytes per second. Sending large graphics files can take tens of seconds. This can be done concurrently with the normal polling traffic along with Telnet diagnostic traffic, but at the cost of system time latency. Nothing prohibits doing large file transfers, but be aware of the time required to push the data through a 9600 bps link. IP addresses associated with this type of traffic should not be placed in the QIP table (see 6.2.4).

6.2.4 High QOS (Quality Of Service) IP Communications

IP packets can be assigned high QOS status. This is performed by storing the IP address in a QIP table. These tables reside in both the master and remote radios. Up to 16 IP addresses can be saved in the QIP table. This table normally contains the IP addresses of hosts that are polling remote RTUs and require low timer latency. RS-232 packets are assigned high QOS by default.

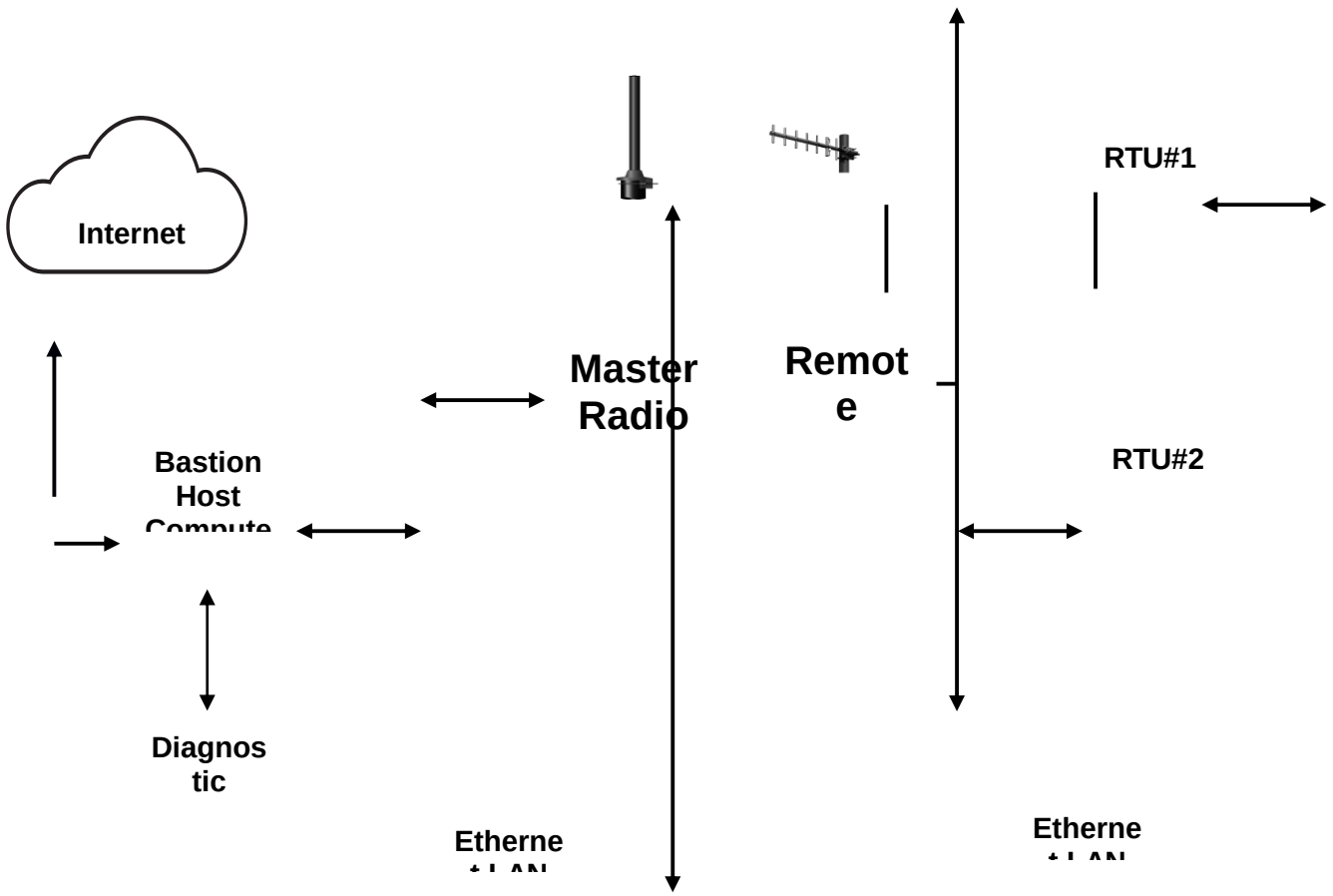


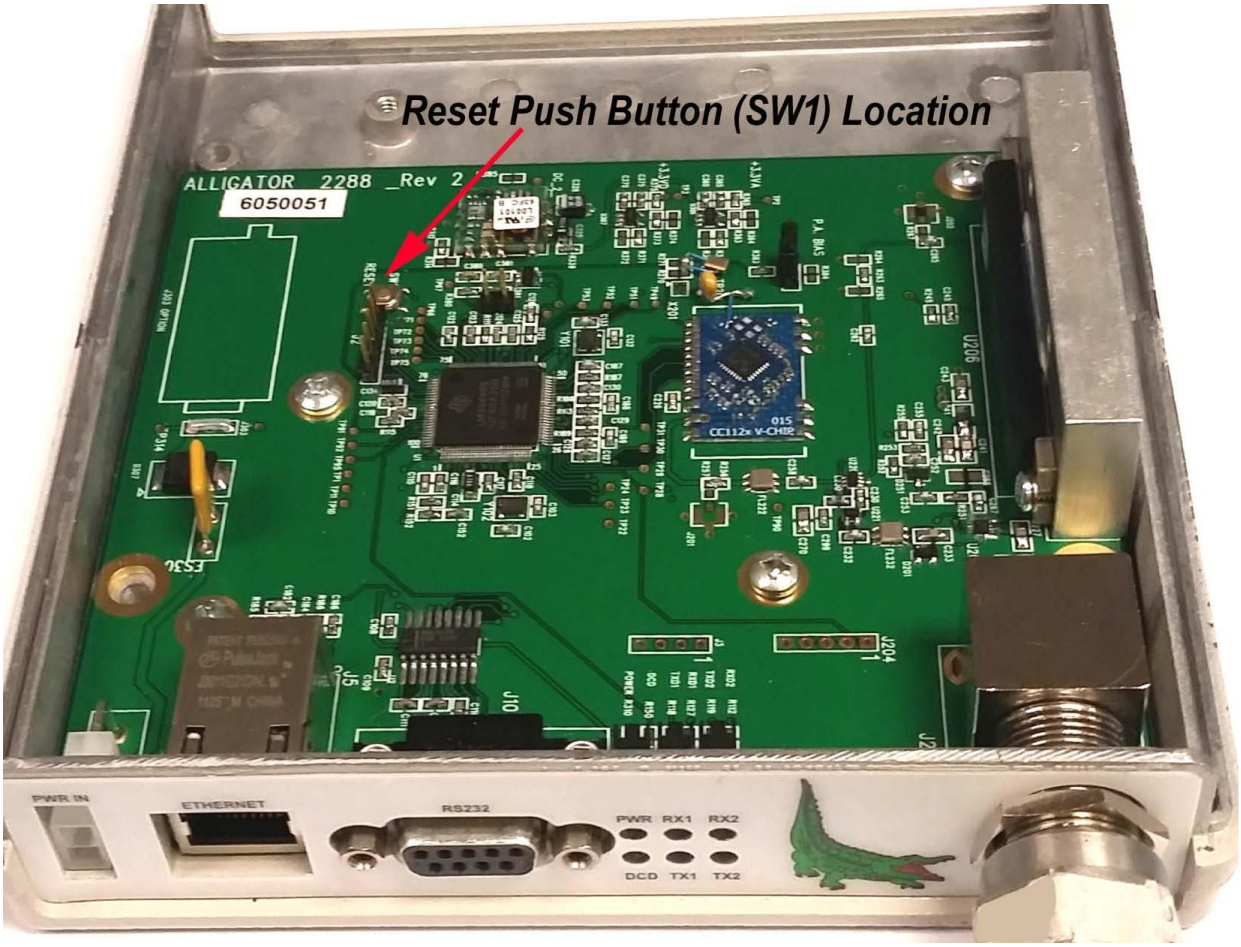
Figure 1 2788 Typical SCADA Block Diagram

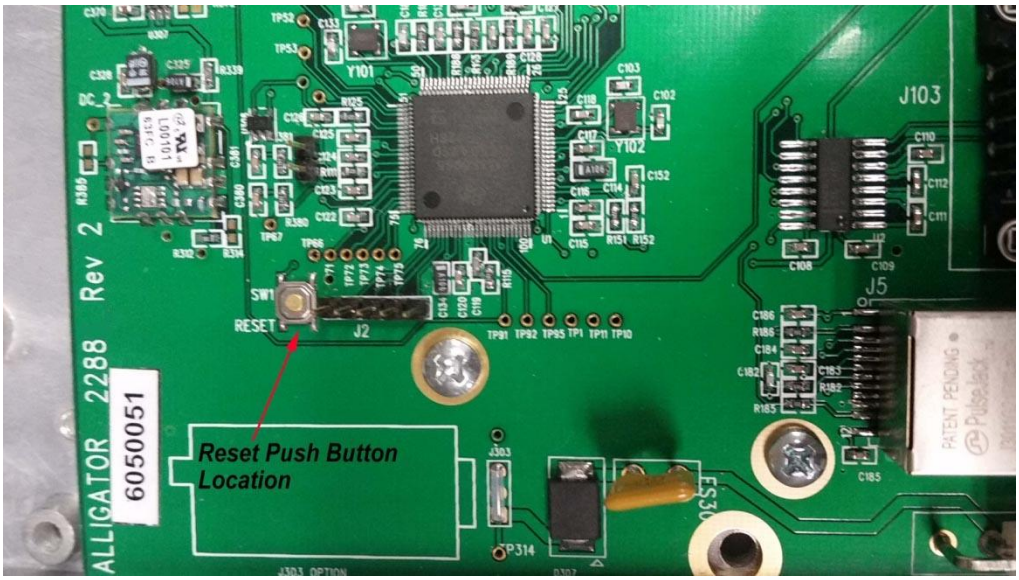
ALLIGATOR COMMUNICATIONS MODEL 2788 LINE USER COMMANDS REV14 06/04/2018

COMMAND	DEFAULT	UNITS	DESCRIPTION
• tf=###.#####<CR>	757.1	MHz	Transmit Frequency (dec point and trailing zeros optional)
• rf=###.#####<CR>	787.1	MHz	Receive Frequency (dec point and trailing zeros optional)
• fc=####<CR>	0	Hz	Frequency Offset Calibration (-10000 to 10000)
• tp=#<CR>	1		Transmit Power 1=low 2=med 3=high
• om=#<CR>	0		Operating Mode 0=remote 1=master
• gc=##<CR>	0		Group Code (0 to 15)
• ip=###.###.###.###<CR>	192.168.1.128		Radio IP Address
• tnp=#####<CR>	23		Radio Telnet Port Number 0 to 65534
• gw=###.###.###.###<CR>	192.168.1.1		Gateway Router IP Address
• sm=###.###.###.###<CR>	255.255.0.0		Subnet Mask
• dr=####<CR>	9600	bps	RS-232 Data Rate 1200, 2400, 4800, 9600, 19200
• ast=####<CR>	120	sec	Anti-streaming time (1 to 4 digits)
• tnt=####<CR>	120	sec	Telnet session activity timer (1 to 4 digits)
• lgt=####<CR>	120	sec	Log-in session activity timer (1 to 4 digits)
• et=#<CR>	1		Enable Transmitter 0=disable 1=enable
• ec=#<CR>	0		Enable Compression (not implemented)
• ee=#<CR>	0		Enable Encryption 0=disable 1=AES256
• ep=#<CR>	0		Enable Password 0=disable 1=enable
• id=###. . .###<CR>	admin		ID word (16 character max, not displayed)
• pw=###. . .###<CR>	password		Password (16 character max, not displayed)
• aesp=###. . .###<CR>	phrase		AES Encryption Phrase (32 character max)
• lo<CR>			Log Out
• q<CR>			Telnet Log Out
• fm=#<CR>	3		Forward Mode 0=rtu&host 1=host 2=rtu 3=all
• rtu0=##-##-##-##-##-##<CR>	00-00-00-00-00-00		RTU0 MAC Address (remote mode)
• rtu1=##-##-##-##-##-##<CR>	00-00-00-00-00-00		RTU1 MAC Address (remote mode)
• rtu[###]=##-##-##-##-##-##<CR>	00-00-00-00-00-00		RTU[n] master MAC Address Table, n hex (000 to 1FF)
• host[#]=##-##-##-##-##-##<CR>	00-00-00-00-00-00		Host[n] MAC Address Table, n hex (0 to F)
• qip[#]=###.###.###.###	0.0.0.0		qip[n] High QOS IP Address Table, n hex (0 to F)
• Escape Key or second Enter key			Print Status
• rtutable<CR>			Print Master RTU MAC Address Table
• qiptable<CR>			Print qip table of high QOS IP addresses
• hosttable<CR>			Print Host MAC Address Table
• lb=##-##-##-##-##-##<CR>	00-00-00-00-00-00		Loopback MAC of Remote Radio (when using dt=5)
• dt=#<CR>	0		Diagnostic Test 0=none 1=TX CW 2=RX CW 3=TX 1 way 4=RX 1 way 5=TX 2 way 6=display TX Buffer 7=display RX Buffer 8=display TX & RX Buffers 9=subpacket

Figure 2 2788 User Line Commands

Model 2788 Internal Reset Push Button Location





FCC Statement

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

The antenna(s) used for this transmitter must be fixed-mounted on outdoor permanent structures.