PAD Operation

Model	CTM-200
Revision	Revision 1.3

Revision Control

| Description	Revision	Date
Customer Release	Revision 1.0	04-Dec-2009
Revised for Chameleon gateways	Revision 1.1	21-June-2011
Updated PAD command format Added note about multiple serial ports	Revision 1.2	20-Jan-2012
Condensed and updated content	Revision 1.3	29-Dec-2015

Contents

1. PAD Operation

Packet Assembly and Disassembly (PAD) is used for sending and receiving "raw" data over IP networks. The Chameleon gateway takes care of establishing IP network connections, as well as the encapsulation of data within UDP or TCP packets. This eliminates the need for a TCP/IP stack running on the host device. This application note details how to setup a Chameleon gateway in PAD mode in order to provide a communications link between a serial port end device and a central control application.

A PAD connection uses the cellular packet data network providing the advantages of higher data rates for quicker response times, and always being connected. PAD mode is typically used for supervisory control and data acquisition (SCADA) applications. PAD mode can be used with master and slave devices that use proprietary communication protocols such as the Allen Bradley DF1 or used to provide direct communications with field devices normally operated on a dial-up modem connection.
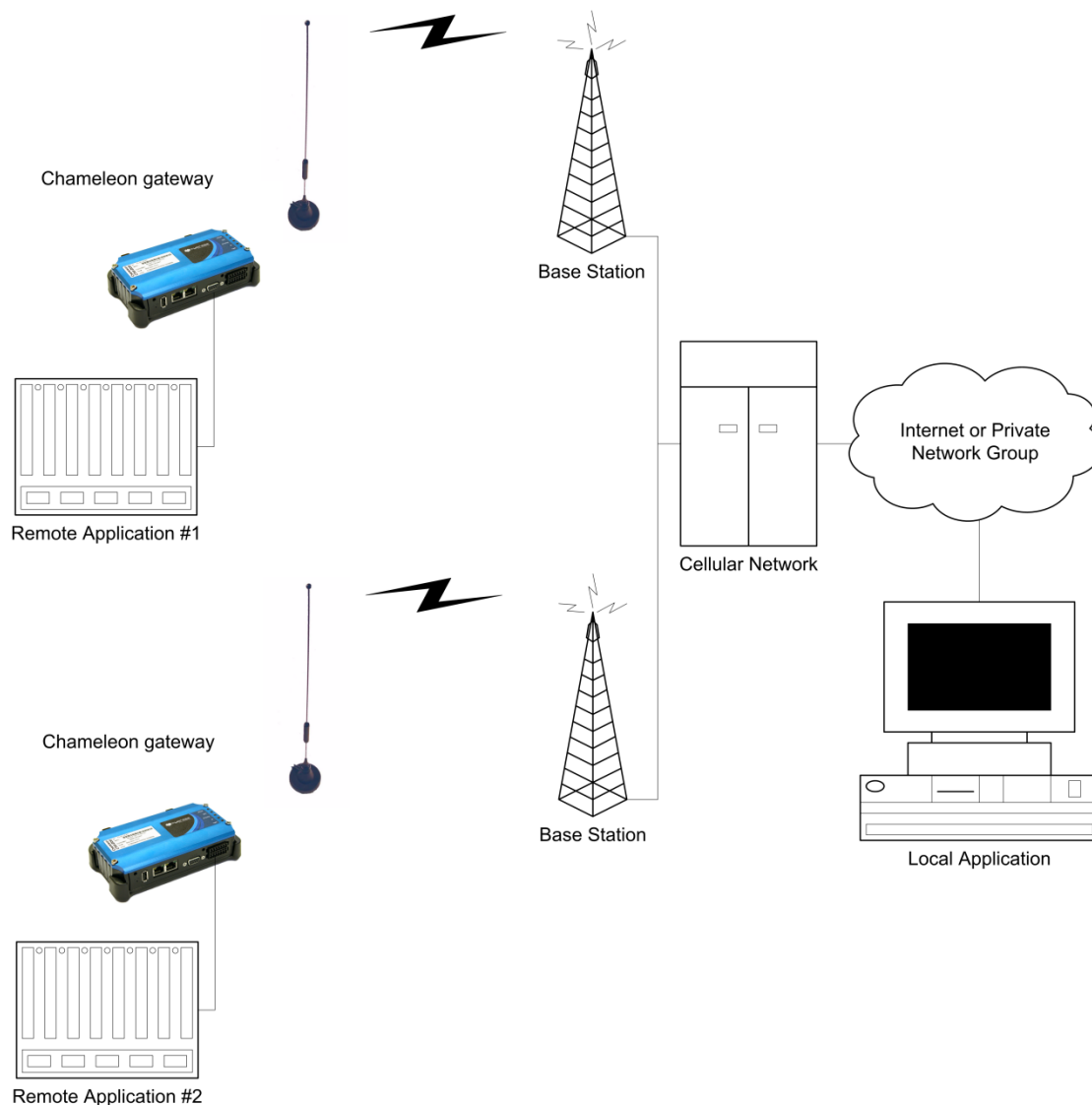
1.1   Selecting the Appropriate PAD Settings

There are two main PAD modes: UDP PAD or TCP PAD.

UDP transport protocol is connectionless and does not guarantee data delivery. However, it is much lighter than TCP in terms of data transmitted. It is considered suitable for the following applications: When total data transfer must be kept to a minimum. Losing a packet is not critical, or the application communication protocol itself provides for retransmissions.

TCP transport protocol is connection oriented and does guarantee data delivery. It will keep trying to send a packet multiple times until its delivery is acknowledged. Because of these characteristics, it has much more overhead compared to UDP. It is suitable for the following applications: When the total amount of data transfer is not critical. Losing a packet is critical and the application communication protocol itself does not perform retransmissions.

Both UDP PAD and TCP PAD can operate in either client or server mode. Client mode means that the gateway is required to establish a connection to a remote device in server mode (this may be through another gateway). Server mode means that the gateway is continually listening on a port and will accept connections from a remote server (this may be from another gateway).

See link to the CTM200 command reference for more details on any commands:
http://www.cypress.bc.ca/documents/Command_Ref/CTM200/

2.   State Diagrams for PAD Operation Modes

The following section provides the state diagrams that describe PAD operation for each of its modes:
- PAD server mode: **cmd pad mode 0** (UDP), **cmd pad mode 1** (TCP)
- PAD client, single-session mode: **cmd pad mode 2** (UDP), **cmd pad mode 3** (TCP)
- PAD client, persistent mode: **cmd pad mode 4** (UDP), **cmd pad mode 5** (TCP)

In the state diagrams below, the circles indicate the current state of PAD and the arrows exiting the circles indicate events which cause PAD to change its state.
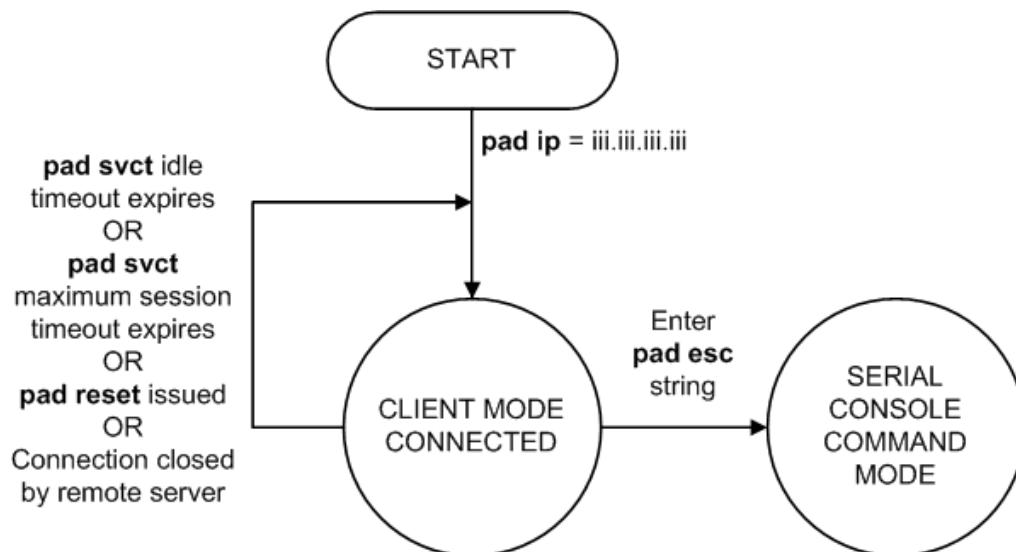
2.1   PAD Server Modes (pad mode 0/1)
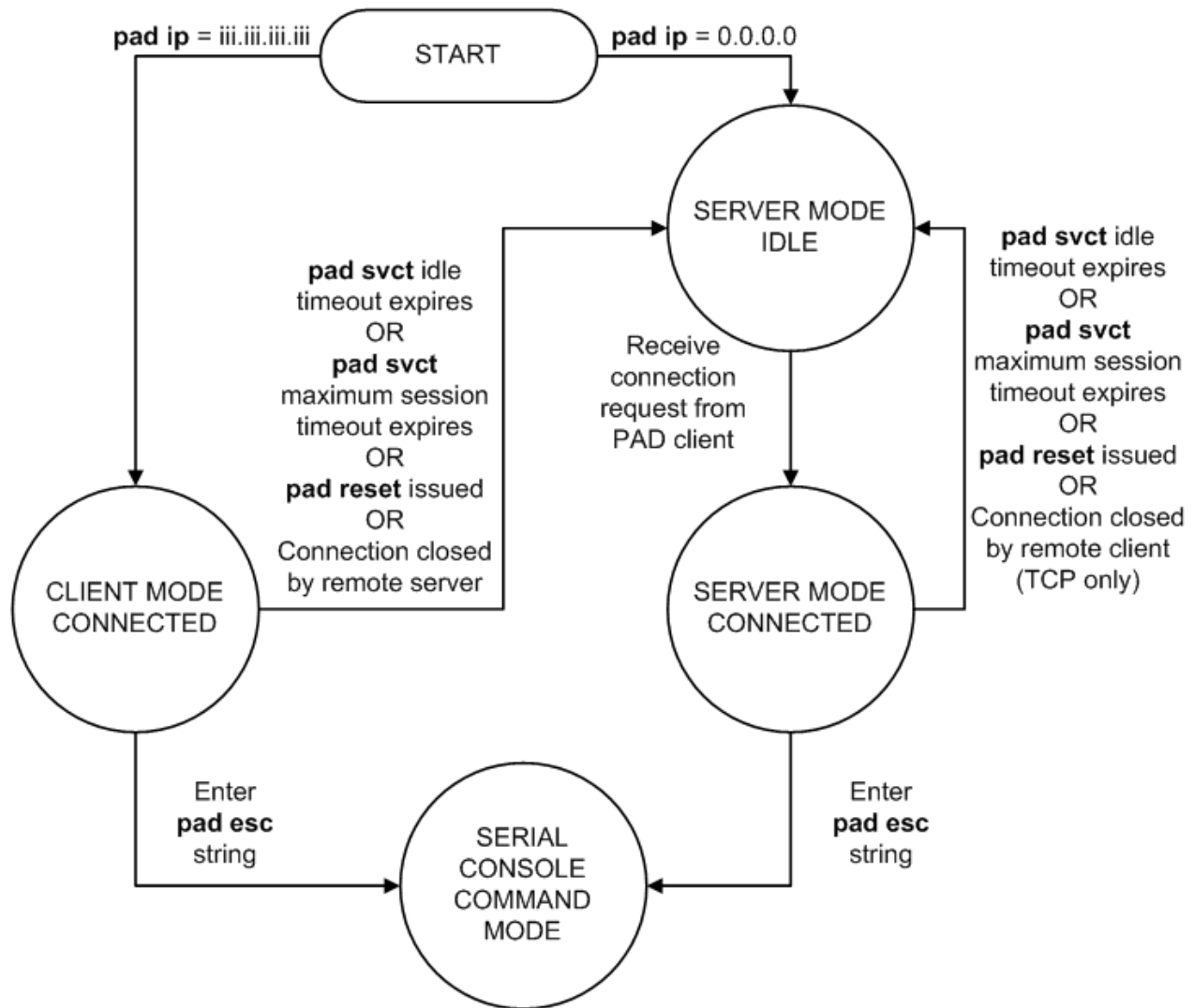
2.2 PAD Client Single Session Modes (pad mode 2/3)
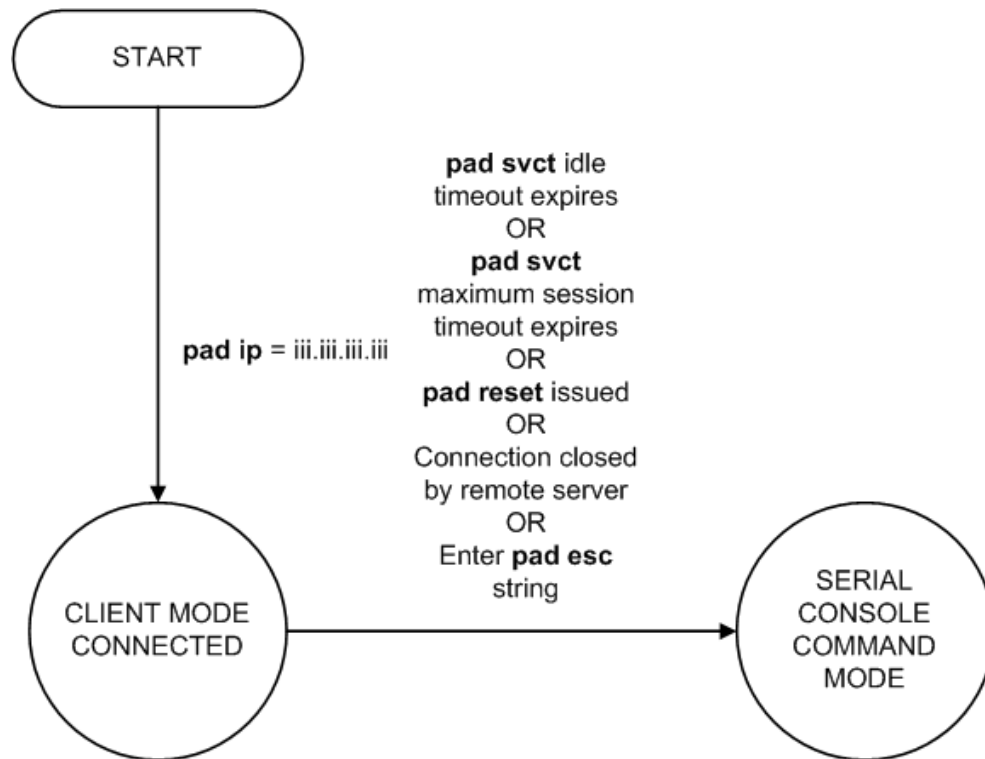
## 2.3 PAD Client Persistent Mode (pad mode 4/5)

3.   Example PAD Configuration

3.1   PAD Configuration for a SCADA Field Device in Slave Mode

In this example, a Chameleon gateway is connected to a SCADA field device which is polled by a remote server. The field device in slave mode is either connected to another Chameleon gateway or has built-in TCP/IP functionality. The field device communicates with a remote server or master device via a request/response protocol. The slave devices will only send responses to requests sent.

The device connected to the gateway's serial port is operating at 9600 baud with no hardware flow control (Tx, Rx, & Gnd signals only), and responds to every incoming sentence with a reply of maximum length 50 bytes of ASCII data always terminated with the character <. The serial slave device does not support echoing of data that it sends to the gateway. The chosen listening port is 5000.
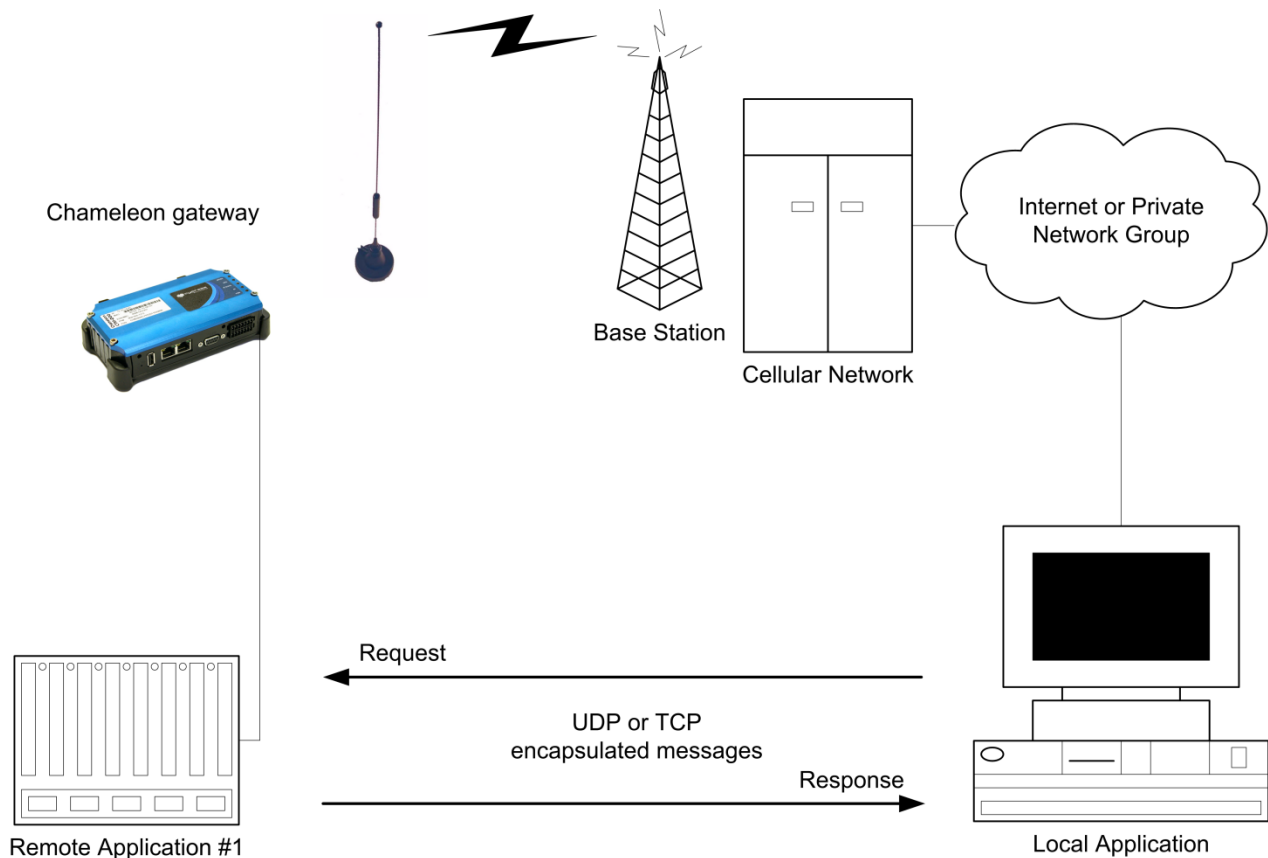
Enter the following commands from the serial console of the gateway connected to the serial slave device:

cmd factory
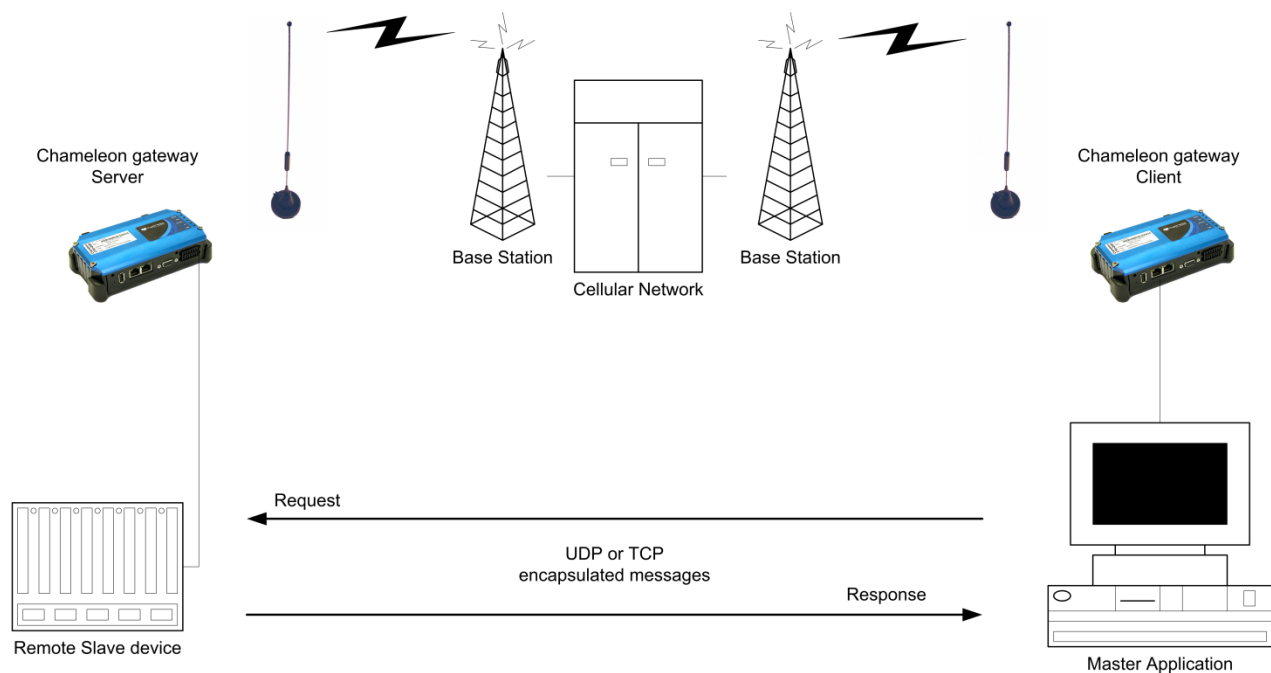**cmd mode 4**
cmd port 1 9600 8 n 1 0
It will now be necessary to adjust the baud rate of the terminal application to 9600.

cmd pad mode 0/1	PAD server mode: 0 = UDP, 1 = TCP
cmd pad echo 0	Do not echo data sent by the slave device back on the serial port
cmd pad ip 0.0.0.0	Sets PAD to server mode only (default settings, in effect after **cmd factory**)
cmd pad port 5000	Sets port on which field device will be listening for requests
cmd pad fwdc 60	Decimal value of ASCII <
cmd pad fwdl 51	Greater than longest message size
cmd pad fwdt 20	Sets the forwarding time to 1 second idle period (default setting, in effect after **cmd factory**)
cmd pad svct 15 0	Set connection timeout to 15 seconds, maximum connection timer is disabled (default settings, in effect after **cmd factory**)
cmd save	Save configuration to gateway's non-volatile memory
cmd pwr mode 2	Power cycle

3.2   PAD Configuration for a SCADA Master Device Polling a Single Field Device in Slave Mode

In this example, a Chameleon gateway is connected to a master device which polls data from a single field device in slave mode. The field slave device is either connected to another Chameleon gateway or has built-in TCP/IP functionality. The master device is typically a server running a SCADA application and communicates with the field device via a request/response protocol. The slave devices will only send responses to requests sent.

The gateway connected to a master device operates at a baud rate of 19200 with full hardware flow control. The master device receives sentences on its serial port of maximum length 100 bytes (with no common end character) which are to be sent to a single slave unit at IP address 100.100.1.2, port 5000. The serial master device requires echoing of data that it sends to gateway.

For the gateway connected to the serial master device, enter the following commands from the serial console:

cmd factory
cmd mode 4
cmd port 1 19200 8 n 1 2
It will now be necessary to adjust the baud rate of the terminal application to 19200.

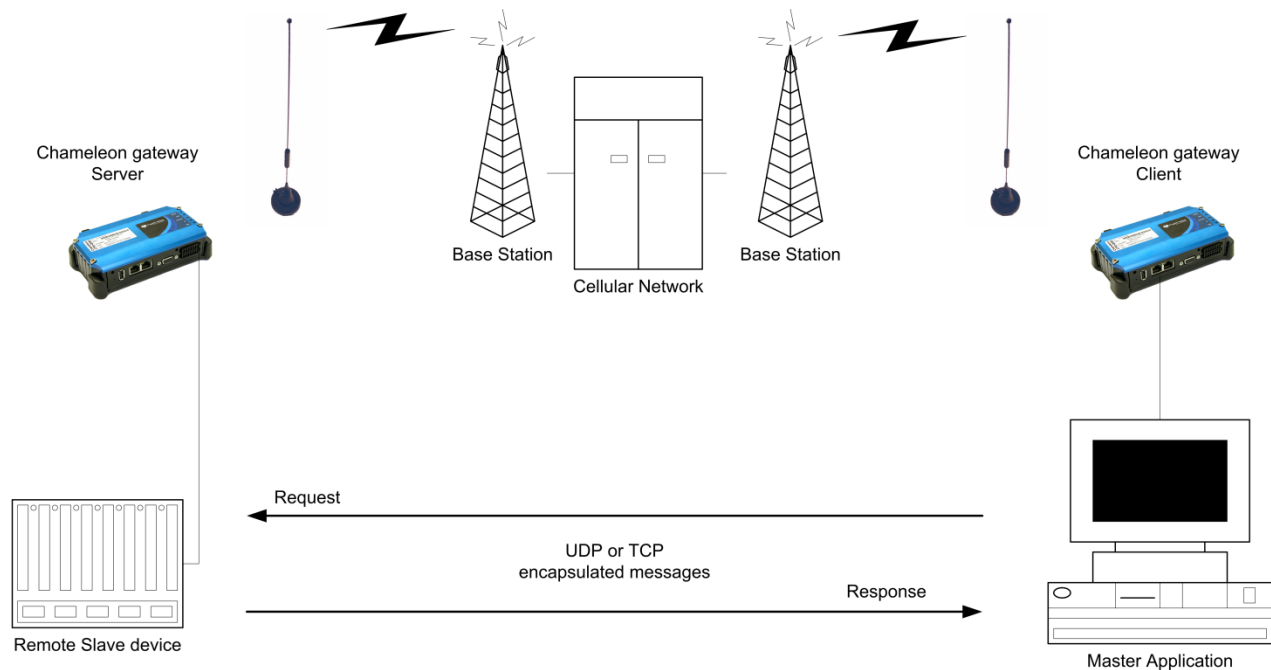|	
cmd pad mode 4/5	PAD client, persistent mode: 4 = UDP, 5 = TCP
cmd pad echo 1	Echo data sent by the master device back on the serial port (default setting, in effect after **cmd factory**)
cmd pad ip 100.100.1.2	Sets IP address of field device being polled
cmd pad port 5000	Sets port of field device being polled
cmd pad fwdc 0	No forwarding character
cmd pad fwdl 101	Greater than longest message size
cmd pad fwdt 10	Sets the forwarding time to 0.5 seconds idle period
cmd pad svct 15 0	Set connection timeout to 15 seconds, maximum connection timer is disabled (default settings, in effect after **cmd factory**)
cmd save	Save configuration to gateway's non-volatile memory
cmd pwr mode 2	Power cycle

3.3   PAD Configuration for a SCADA Master Device Polling Multiple Field Devices in Slave Mode

In this example, a Chameleon gateway is connected to a programmable master device intended to poll multiple field devices in slave mode. The master device is typically a server running a custom SCADA application and communicates with field devices via a request/response protocol. The slave devices will only send responses to requests sent.

The gateway is connected to a master device at baud rate of 19200 with full hardware flow control. It receives sentences on its serial port of maximum length 100 bytes (with no common end character) which are to be sent to multiple slave units at IP addresses 100.100.1.1-100.100.1.10, port 5000. The slave devices typically respond within 8 seconds. The serial master device requires echoing of data that it sends to the gateway. In this example, the master device requires built-in scripting functionality to perform predefined actions based on serial port output when in command mode.

Enter the following commands from the serial console of the gateway connected to the serial master device:

cmd factory
cmd mode 2
cmd port 1 19200 8 n 1 2
It will now be necessary to adjust the baud rate of the terminal application to 19200.

cmd pad mode 2/3	PAD client, single-session mode: 2 = UDP, 3 = TCP
cmd pad echo 1	Echo data sent by the master device back on the serial port
	(default setting, in effect after **cmd factory**)
cmd pad fwdc 0	No forwarding character
cmd pad fwdl 101	Greater than longest message size
cmd pad fwdt 100	Sets the forwarding time to 5 seconds idle period
cmd pad svct 10 0	Set connection timeout to 10 seconds, maximum connection timer disabled
cmd save	Save configuration to gateway's non-volatile memory
cmd pwr mode 2	Power cycle

In command mode, for each request to a specific slave device, the master device should send the following commands:

|	
cmd pad ip 100.100.1.1	Sent by master device to set new PAD slave to which to connect
cmd freeconsole	Kills current serial console shell processes
cmd gopad	Sent by master device to start new PAD connection

Upon executing **cmd gopad**, the gateway will connect to the PAD slave with IP address **100.100.1.1** as specified in **cmd pad ip**, transmit a request, and disconnect if the connection idle time is 10 s, or if the escape sequence is entered on the serial port (default is **+++**). Once disconnected, the gateway will drop into command mode. Repeat **cmd pad ip** and **cmd gopad** for other slave devices using IP addresses **100.100.1.2**-**100.100.1.10**.

In this example, the master device requires some scripting or programmable functionality to perform the following actions iteratively for polling data from slave devices:

1. Detect the gateway's command mode by checking that the pound character (**#**) is received on the serial port
2. Execute **cmd pad ip** using the field device's IP address
3. Execute **cmd pad port** using the field device's port
4. Execute **cmd gopad** to start PAD operation
5. Send the current field device request over the serial port
6. Wait for the response from the field device. In this example, the gateway should drop back into command mode after 10 seconds.

3.4   PAD Configuration for a Reporting Field Device

In this example, a Chameleon gateway is connected to a field device that reports to a remote server without the need to be polled. The field device generates data on the serial port whenever it is available and the gateway will send this data remotely over-the-air. The remote field device operates at a baud rate of 9600 and uses hardware flow control. The field device generates ASCII data with varying length and is always terminated with the carriage return character <CR>. The field device does not require echoing of data that it sends to the gateway.
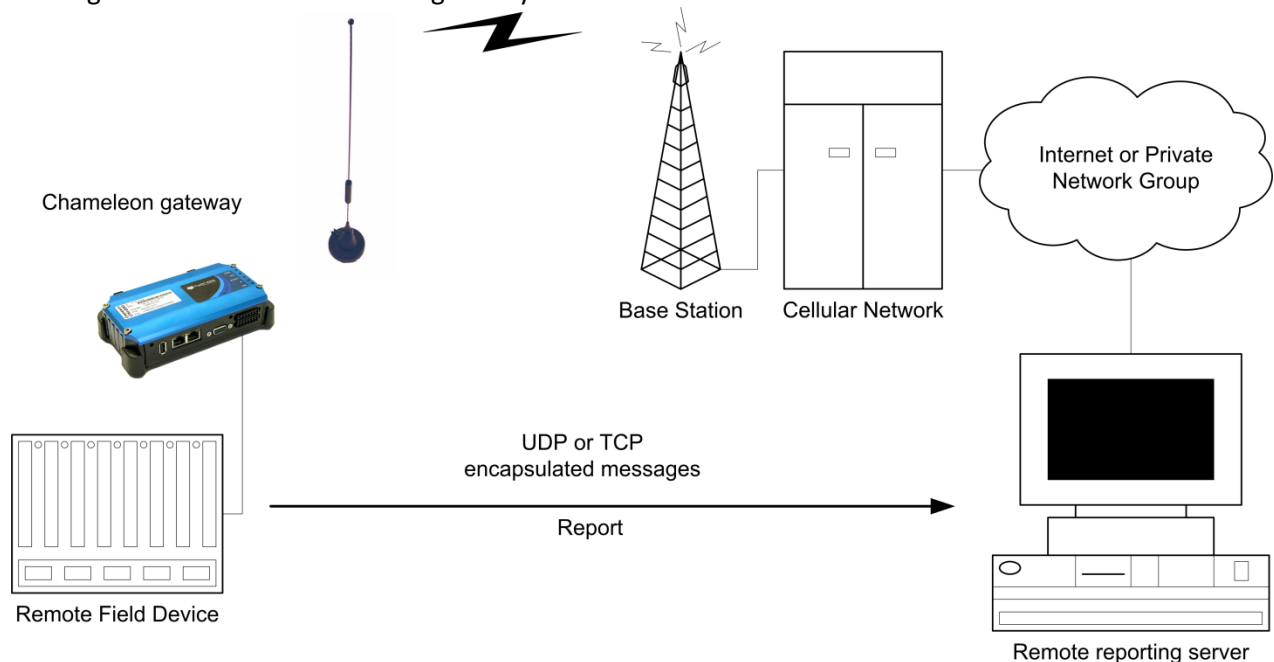
For the gateway connected to the reporting field device, enter the following commands from the serial console:

cmd factory
cmd mode 4
cmd port 1 9600 8 n 1 2

It will now be necessary to adjust the baud rate of the terminal application to 9600.

cmd pad mode 4/5   PAD client, persistent mode: 4 = UDP, 5 = TCP
cmd pad ip 200.100.1.1 Sets IP address of remote server handling data reported by the field device
cmd pad port 8000   Sets port to which data is to be sent
cmd pad echo 0   Do not echo data sent by the field device back on the serial port
cmd pad fwdc 13   Decimal value of ASCII <CR> (default setting, in effect after **cmd factory**)
cmd pad fwdl 40   Data to be sent over the air in 40-byte packets or less if <CR> in first 40 bytes
                          (default setting, in effect after **cmd factory**)
cmd pad fwdt 20   Sets the forwarding time to 1 second idle period
                          (default setting, in effect after **cmd factory**)
cmd pad svct 15 0   Set connection timeout to 15 seconds, maximum connection timer is disabled
                          (default settings, in effect after **cmd factory**)
cmd save   Save configuration to gateway's non-volatile memory
cmd pwr mode 2   Power cycle

Technical Support

**Cypress Solutions Service
Support Group**
1.844.462.9773 or 778.372.4603
9.00am to 5.00pm PST
support@cypress.bc.ca