# Digi Cellular Gateway Security Overview

## Introduction

This document discusses security topics related to Digi cellular gateways (a.k.a. routers) such as the Digi Connect® WAN, ConnectPort™ WAN and ConnectPort™ X gateway families (but not including the Digi Wi-Point 3G™). The document is divided into four main sections:

1. Securing access to the Digi gateway itself
2. Securing data traffic through the Digi gateway
3. Wireless provider security options
4. A note on PCI compliance

More information is available in the Digi cellular gateway *User's Guide* and *Command Reference* available from http://www.digi.com/support and on the product CD. Online help is also available via the Digi device's built-in WebUI "help" icon in the upper right of each screen. Command line assistance is available by using a question mark "?" for syntax help; for example "set service ?" to see a list of options for the set service command. (Note CLI commands can usually be abbreviated. For example, "display passthrough" can be abbreviated "dis pass".)

## Contents

# 1 Securing the Digi Gateway

## 1.1 Physical Security

The first and most important aspect of securing a device is to physically secure the device itself, preferably under lock and key. This is especially true with a cellular device since it will work in most any location. Digi gateways have various mounting options that can help deter theft.

However, securing the device in a “hard-to-reach” location such as a wiring closet can defeat the idea of placing the Digi device where it gets a better signal. It is typically easier and less expensive to run Ethernet cable vs. running longer antenna coax, especially for devices that use two antennas. The Digi gateway can still typically be mounted securely using screws to discourage theft even when placed in an area close to a window or outside wall.

Placing the Digi gateway in a secure location can also prevent visual inspection of the front panel signal and link LEDs. So, you must weigh security vs. accessibility and cost and complexity of installation. Signal information is available via the Digi device’s WebUI and command line.

Keep a list of Digi MAC addresses and/or device IDs*, ESNs/IMEIs (modem serial numbers) and/or SIM IDs as required so that devices can be disabled in the event of theft. (* Digi Connectware Manager is a tool that can help track devices and determine if a device is active. Digi Connectware Manager uses the device ID, which is derived from the MAC address, as its database key.)

Antenna security is also important. Mount external antennas securely to prevent theft and weather damage. Non-obtrusive, low-profile antennas are available from various sources.

For multi-port devices like the ConnectPort WAN, there are RJ45 blocking devices such as the Panduit PSL-DCJB that can prevent plugging in a cable.

## 1.2 Securing Access to the Digi Device

Security-related features in Digi cellular products include:

1. Secure access and authentication:
    - One password, one permission level.
    - Can issue passwords and SSH keys to device user.
    - Can selectively enable and disable network services such as ADDP, RealPort, Encrypted RealPort, HTTP/HTTPS, LPD, Remote Login, Remote Shell, SNMP, and Telnet.
    - Can control access to inbound ports.
    - Secure sites for configuration: HTML pages for configuration have appropriate security.
    - IP Filtering / Access Control List support.

2. Support for X.509 Digital certificates for IPsec VPN and SSL.Encryption:
    - Strong Secure Sockets Layer (SSL) V3.0/ Transport Layer Security (TLS) V1.0-based encryption: DES (64-bit), 3DES (192-bit), AES (128-256-bit).
    - IPsec ESP: DES, 3DES, AES.
    - Encrypted RealPort® is available for IP connections between the COM/TTY port(s) on the Digi cellular device to the server on which the RealPort driver is installed.

3. SNMP security:
    - Authorization: Changing public and private community names is recommended to

prevent unauthorized access to the device.
- SNMP “set” commands can be disabled to make use of SNMP read-only.

### 1.2.1 Note about IP Pass-through Mode

As described in the “Securing Data Traffic through the Digi Gateway” section below, the Digi gateway has two primary modes of operation:

1. Router using Network Address Translation (NAT) with optional IPsec VPN
2. IP Pass-through mode, which is essentially bridging, where the mobile IP address and all incoming cellular traffic are forwarded through to a device such as a router or VPN appliance connected via Ethernet. In this mode, the main security concerns on the Digi device itself are management pinholes to allow WebUI or command line access to the Digi device itself.

   *WebUI*: See Configuration > Network > IP Pass-through

   *Command Line*: “`set passthrough`”.

▶ *In IP Pass-through mode, most all security is the responsibility of the Ethernet device (e.g., router or VPN appliance) connected behind the Digi gateway*.

### 1.2.2 Local Serial Port Access

Digi cellular gateways have one or two serial ports. By default, these ports are enabled for local command line (CLI) access. Access to these ports can be restricted as follows:

- Disable serial port CLI access altogether by changing the port *profile* to something other than “Local Configuration” or “<unassigned>”:

  *WebUI*: Configuration > Serial Ports

  *Command Line*: “`set profile`”

  *Note*: If the profile is changed, the Digi device must either be rebooted or the local serial port session must be killed manually. See the “who” command information listed later in this document.

- To still allow access to the CLI, but make it more secure, change the serial port communications settings from the default settings of 9600, 8, 1, N to something difficult to guess (e.g. 57600, 7, 1, Odd).

  *WebUI*: Configuration > Serial Ports > Basic Serial Settings

  *Command Line*: “`set serial`”

- Enable user name and password as described below.

### 1.2.3 Assign a User Name, Password and Optional SSH User Key

The first and simplest way to secure command line and WebUI access is to assign a user name and password. By default no password is required. The default user name is “root”.

*WebUI*: Configuration > Security. Change the User Name as needed. Click to “Enable password authentication” and enter the password. Optionally, enter an SSH encryption to be used with SSH client connections to the Digi device.

*Command Line*:

Change user name: "`set user name=[new_user_name]`". "`set user`" can also be used to load an SSH key. See "`set user ?`" or the Command Reference for details.

Issue new password: "`newpass`". `newpass` is interactive and will prompt for the old password and then new password.

### 1.2.4 Changing LAN IP Address and DHCP Settings

You may want to prevent access to the Digi device or outbound communication by limiting the Digi device's IP address range and DHCP server options. By default the IP address is 192.168.1.1 and DHCP server is on. For example:

- Change the **LAN IP address and subnet** to something hard to guess other than 192.168.1.0 which is the most commonly used SOHO subnet. Select an IP setup such as 172.33.25.9/255.255.255.252. This effectively locks down the device to just a few IP addresses that can access the device.

  DHCP client is off by default (and should remain off is most situations).

  *WebUI*: Configuration > Network > IP Settings

  *Command Line*: "`set network ip=(ipaddr) submask=(subnet mask) gateway=(gateway ipaddr)`"

- **Disable AutoIP** (on by default) which will prevent the Digi device from assigning itself an address in the 169.254.n.n range if the Digi device's DHCP client is enabled.

  *WebUI*: Configuration > Network > Advanced Network Settings > IP Settings > clear the "Enable AutoIP" check box.

  *Command Line*: "`set network autoip=off`"

- **Disable DHCP Server** (on by default) or use the Static Lease reservations to limit which client devices can obtain IP addresses.

  *WebUI*: Configuration > Network > DHCP Server Settings

  *Command Line*: "`set dhcpserver`"

### 1.2.5 Configure IP Services

Digi cellular gateways use TCP and UDP IP services for various functions such as command line access via telnet or SSH, remote management, and direct access to serial ports via TCP or UDP. You can disable services or change the TCP/UDP ports used by these services.

Below is a table of all the TCP/UDP services used on a Digi gateway with an explanation of the service. Not all the listed service ports are used in all Digi configurations and vary by model and firmware versions; for example a Digi Connect WAN has only one serial port, thus only serial one port is listed in its "show service" listing.

| Protocol | Port(s) | Service/Function/Notes |
|---|---|---|
| **The following services are for management of the Digi gateway** | | |
| TCP | 22 | SSH Server for command line access |
| TCP | 23 | TELNET Server for command line access |
| TCP | 80 | HTTP server for on-board WebUI (note the HTTP and HTTPS server are tied together, disabling one will disable both) |
| UDP | 161 | SNMP |
| TCP | 443 | HTTPS server for secure WebUI access (note HTTP and HTTPS server are tied together, disabling one will disable the other) |
| TCP | 513 | RLOGIN Server |
| TCP | 514 | RSH Server |
| UDP | 2362 | ADDP Digi device discovery protocol used by Digi discovery wizards/tools |
| TCP | 3197 | Digi Connectware Manager TCP client (for device initiated remote management connections; cannot be disabled or changed) |
| TCP | 3198 | Digi Connectware Manager TCP server (for server initiated remote management connections; cannot be disabled or changed) |
| **The following services are for access to Digi gateway serial ports and other non-management functions** | | |
| TCP | 7 | TCP_ECHO (diagnostics only) |
| UDP | 7 | UDP_ECHO (diagnostics only) |
| UDP | 500 | IKE/ISAKMP (cannot be disabled or changed) |
| TCP | 502 | Modbus/TCP (Digi Connect WAN IA only) |
| TCP | 515 | LPD Server |
| TCP | 771 | RealPort server (COM/TTY port redirection) for serial port connections |
| TCP | 1027 | Encrypted RealPort server (COM/TTY port redirection) for serial port connections |
| TCP | 1080 | SOCKS protocol proxy (Digi Connect WAN family only) |
| TCP | 2001-2002 | Reverse telnet server listening for ASCII socket to serial ports 1-2 |
| TCP | 2101-2102 | TCP server listening for raw socket to serial ports 1-2 |
| UDP | 2101-2102 | UDP server listening for raw UDP connections to serial ports 1-2 |
| TCP | 2501-2502 | Reverse SSH server listening for socket to serial ports 1-2 |
| TCP | 2601-2602 | SSL server listening for socket to serial ports 1-2 |
| TCP | 4401 | Socket tunnel; used with TCP or SSL socket tunnels |
| TCP | 50000 | Modem emulation (pseudo modem) pool for first available port |
| TCP | 50001-50002 | Modem emulation (pseudo modem) TCP server on ports 1-2 |

Please refer to the “show service” command for updates and details specific to your Digi gateway and firmware.

How to change service settings:

*WebUI*: Configuration > Network > Network Services Settings

*Command Line*: “`show service`” to see a list of services and ports (see below); “`set service index=[index] state=[on|off] ipport=[network port number]`” to change ports or to disable services.

Here is a sample list of the IP service ports used by a ConnectPort WAN VPN firmware version 2.6.0.10:

```
#> show service

 Service Configuration :

 index state ipport keepalive nodelay dlyd-ack                        service
     1   off      7       off     off      200                TCP Echo Service
     2   off      7        na      na      200                UDP Echo Service
     3    on     22       off     off      200                     SSH Service
     4    on     23       off     off      200                  Telnet Service
    22    on     80        na      na      200                    HTTP Service
    23    on    161        na      na      200                    SNMP Service
     5    on    443        na      na      200                   HTTPS Service
    25   off    513       off     off      200                  Rlogin Service
    26   off    514       off     off      200                     Rsh Service
    18   off    515       off     off      200             Line Printer Daemon
    17    on    771       off      na      200                RealPort Service
     6    on   1027       off      na      200      Encrypted RealPort Service
     7    on   2001       off     off      200          Telnet Server (Port 1)
     8    on   2002       off     off      200          Telnet Server (Port 2)
     9   off   2101       off     off      200             TCP Server (Port 1)
    11   off   2101        na      na      200      Serial/UDP Server (Port 1)
    10    on   2102       off     off      200             TCP Server (Port 2)
    12    on   2102        na      na      200      Serial/UDP Server (Port 2)
    24    on   2362        na      na      200                    ADDP Service
    13    on   2501       off     off      200             SSH Server (Port 1)
    14    on   2502       off     off      200             SSH Server (Port 2)
    15   off   2601       off     off      200  Secure Socket Service (Port 1)
    16    on   2602       off     off      200  Secure Socket Service (Port 2)
    27   off   4401        on     off      200            Socket Tunnel Server
    19    on  50000        na      na      200          Modem Emulation (Pool)
    20    on  50001       off     off      200        Modem Emulation (Port 1)
    21    on  50002       off     off      200        Modem Emulation (Port 2)
```

For example you may wish to prohibit the ability of someone on the local LAN to use Digi’s device discovery tool, which uses the ADDP protocol, to find the Digi device’s Ethernet interface IP address. Digi devices listen on UDP port 2362, the ADDP port, and respond with its IP address to multicast messages sent by the discovery application. Use the “`show service`” command to verify status of current services; then use “`set service index=24 state=off`” to turn off the ADDP protocol listening service.

### 1.2.6 Note about Telnet and Rlogin Embedded Client

Digi gateways have telnet and rlogin clients available from the command line interface (CLI). These clients *cannot be disabled*. It is important to secure access to the CLI by preventing unwanted access:

(a) Enable user-name/password,

(b) Change/disable TCP services, and
(c) Configure IP Filtering.

These can help prevent someone from hopping from the Digi to another network node via telnet or rlogin.

### 1.2.7 Configure IP Filtering / Access Control List

IP Filtering (also called Access Control List or ACL) is a security feature that provides blocking of specific incoming, i.e., mobile terminated traffic, into the Digi gateway except for traffic from specific IP addresses and/or subnets as defined in the IP filtering configuration. There are three IP filtering sections on the Digi device:

1. Only allow access from the following devices and networks. When checked this blocks ALL incoming traffic except for the traffic from the IP address/subnets listed in the "allow access" tables (see 3 below).
2. Automatically allow access from all devices on the local subnet. This allows outbound traffic from the private Ethernet network out to the mobile network and beyond.
3. When the "Only allow access from the following devices and networks" box is checked, entries must be added to allow incoming mobile traffic to be passed through the Digi device to the Ethernet network. Entries are allowed for subnets and/or individual host addresses.

**CAUTION**: Incorrect settings here can block some or all traffic, even traffic originated from the LAN. For example, checking "Only allow access from the following devices and networks" without adding IP addresses or subnets to the "allow access" tables will block ALL incoming traffic including responses to outgoing requests.

The Digi gateway does *not* contain a *stateful* firewall. That is, it does not maintain a state table of out-going connections. For example, you attempt to open www.digi.com, but the IP address of www.digi.com is not in the "allow access" table; therefore, responses back from www.digi.com are blocked.

Configuring IP Filtering / Access Control:

*WebUI*: Configuration > Network > IP Filtering Settings

*Command Line*: "`show accesscontrol`" to see a list of current settings;
"`set accesscontrol [enabled={on|off}] [autoaddsubnets={on|off}] [addrip[1-64]=ipaddress] [subnip[1-32]=ipaddress] [subnmask[1-32]=mask]`"
to change ports or to disable services.

### 1.2.8 Configure SNMP

SNMP is supported on all Digi gateways. SNMP has the obvious advantages of providing feedback and control to/from network management systems. However, SNMP can also be a security risk.

Disable SNMP: SNMP can be disabled if network management is not being used.

*WebUI*: Configuration > Network > Network Services Settings, or
Configuration > System > SNMP Settings

*Command Line*: "`set service index=[index*] state=off`" (* normally 23, use "show service" to verify).

SNMP can be made more secure by changing settings. The Public community and Private community fields specify passwords required to get or set SNMP-managed objects. Changing public and private community names from their defaults of “public” and “private” respectively is recommended to prevent unauthorized access to the device.

The “Allow SNMP clients to set device settings through SNMP” checkbox enables or disables the ability for users to issue SNMP set commands.

SNMP settings can be configured via:

*WebUI*: Configuration > System > SNMP Settings

*Command Line*: “`set snmp [trapdestip=ipaddress publiccommunity=string privatecommunity=string setsenabled={on|off} authfailtrap={on|off} coldstarttrap={on|off} linkuptrap={on|off} logintrap={on|off}]`”

### 1.2.9 Display Current Status and Sessions

The following CLI commands show current status and connections:

- `display netdevice`
- `display sockets`
- `display udp`
- `display tcp`
- `display route`
- `display arp`
- `display proxyarp`
- `display ppp`
- `display passthrough`
- `display mobile`
- `display accesscontrol`
- `display nat`
- `show vpn all`
- `display vpn`
- `dhcpserver status`
- `display log`
- `who`

The last command listed, “`who`” (which is also available in the WebUI via Management > Connections), shows current mobile connections, user CLI sessions and Digi Connectware Manager remote management sessions. ConnectPort WAN VPN example:

```
#> who

ID  From                  To                    Protocol              Sessions
--  --------------------  --------------------  --------------------  --------
1   serial 1              local shell           term
2   serial 2              local shell           term
3   70.12.94.n            68.28.153.69          ppp [connected]
4   70.12.94.n:43846      66.77.174.n:3197      connectware tcp
5   172.16.5.106          local shell           telnet
```

This listing shows:

- IDs 1-2: local serial port CLI sessions
- ID 3: The mobile PPP session to the carrier network

- ID 4: Digi Connectware Manager TCP session
- ID 5: Telnet CLI session

A session can be killed (including the mobile connection) using:

*WebUI*: Management > Connections > Disconnect

*Command Line*: "`kill <ID>`"

Note that WebUI sessions are *not* listed via `who` or WebUI Management > Connections.

### 1.2.10 Digi Connectware Manager and Security

Digi Connectware Manager remote management traffic to/from the Digi device can be secured and uses a proprietary protocol. User access to Digi Connectware Manager itself is typically via HTTPS. Various user-levels exist to provide various levels of security.

As noted above, Digi Connectware Manager uses TCP ports 3197 or 3198. These are reserved ports and use proprietary Digi protocols. These ports cannot be disabled, but will not be used unless the Digi device is enabled for Remote Management.

Refer to Digi Connectware Manager Implementation Guide for details.

# 2 Securing Data Traffic *Through* the Digi Gateway

As mentioned earlier, most Digi router models have three primary modes of operation:

1. Router using Network Address Translation (NAT), which is the default mode,
2. IP Pass-through mode, which is essentially bridging, or
3. Accessing remote devices via the built-in serial port(s).

As noted above, data security in IP Pass-through mode is mainly the responsibility of the router or VPN device connected behind the Digi gateway via Ethernet. The only security settings in IP Pass-through mode are for the management pinholes. Therefore, this section focuses entirely on *Router/NAT* mode.

NAT is enabled by default when the Digi gateway is in routing mode. NAT should remain enabled except in rare cases where a private wireless plan is being used and static routes can be added to the Digi gateway or Internet routable IP addresses can be used on the remote LAN connected to the Digi.

NAT adds a level of security itself by blocking any unsolicited inbound traffic (except for service traffic to the Digi itself). Traffic destined for hosts connected behind the Digi gateway via Ethernet can be forwarded via these methods:

- TCP/UDP port forwarding where traffic is forwarded based on a specific TCP/UDP port number to a host or serial port.
- GRE protocol forwarding
- IPsec ESP protocol forwarding
- SSL tunnel/forwarding
- IPsec VPN termination/initiation.

Care must be taken when using any of these methods, especially TCP/UDP forwarding, to avoid forwarding unwanted traffic to a host listening on a particular port. For example, telnet traffic on port 23 is disabled on the Digi gateway, but is supposed to be forwarded to a router at IP 192.168.1.2. The IP address is mistyped in the IP forwarding configuration as 192.168.1.3 which is a Linux server controlling a critical function.

And, of course, security must be properly configured on the terminating device as well as the Digi gateway itself. For example, enable username/password authentication on the connected device.

TCP/UDP inbound ports can be different from the outbound port. For example for telnet, use port 9923 for the source address, but destination port 23 to the router. This adds a simple level of security by requiring a port scan or guessing to find the port being used.

GRE and IPsec ESP protocols can be forwarded in similar fashion – again, care must be taken to properly configure Digi gateway forwarding as well as the security of the device terminating the GRE or IPsec ESP connection.

See also "**IP Filtering**" above to block all incoming traffic except for networks and hosts defined in the access control list (ACL). This will also block any responses to outbound requests that are not listed in the ACL.

## 2.1 Secure Socket (SSL) Tunneling

Data traffic to/from a host can be encrypted/decrypted using simple SSL tunneling and DES, 3DES or AES encryption. This can be used to secure ATM or similar transactions. This support is for only one host / one TCP port.

*WebUI*: Configuration > Network > Socket Tunnel Settings

*Command Line*: "`set socket_tunnel`"

## 2.2 IPsec VPN

Network traffic can be protected using native IPsec ESP VPN built into most Digi gateway models, such as the ConnectPort WAN VPN. The Digi gateway IPsec implementation is a standard network device implementation supporting the following:

1. Manual Key VPN
2. Auto-Key IKE VPN using pre-shared keys or X.509 digital certificates
3. MD5 and SHA1 hash algorithms
4. DES, 3DES and AES encryption (AES encryption to 256-bits)
5. Split tunnel or tunnel-all modes

*WebUI*: Configuration > Network > VPN Settings

*CLI*: See "set vpn"

## 2.3 Secure Out-of-band Console Management Access

A unique feature of most Digi cellular gateways is the ability to use the serial port(s) for out-of-band access to console ports remote routers, VPN appliances, etc. Here, CLI access is "passed through" to the serial port via reverse telnet or SSH traffic by enabling the "Console Management" serial port profile. As shown above under "IP Services" the default ports of 2001-2002 for telnet and 2501-2502 for SSH can be changed or disabled. SSH provides the most secure mechanism since it requires authentication to the Digi device itself before it passes the connection to the serial port.

## 2.4 Secure Serial Port Communications

In addition to being used for console management as mentioned above, most Digi cellular routers/gateways have serial ports that can be used for communications to/from serial devices like RTUs, PLCs, data loggers, monitors, etc. The Digi serial ports can be used in several modes such as TCP server or client, RealPort, Modbus, or serial bridge. In most cases, one uses the Mobile IP address and a specific TCP port number to connect through the Digi device directly to

the serial port. There are four ways to protect traffic to/from serial ports:

1. Encrypted RealPort: RealPort is Digi's patented COM/TTY port redirection driver. The Digi device and driver have the ability to encrypt the traffic using SSL/TLS. There are settings on the Digi device and RealPort driver to enable this.
2. SSL: Here traffic is encrypted and authenticated via SSL socket.
3. SSH: SSH is normally used for "console" CLI access.
4. IPsec VPN: IPsec can be used to protect serial port traffic just as it can normal IP Ethernet to mobile interface traffic. However, the application will use the Digi device's Ethernet address vs. the mobile IP address to access the serial port. Due to the complexity and overhead of IPsec, any of the above methods are recommended instead. IPsec would be good to use if Ethernet traffic is also being secured.

### 2.5 Block Carrier DNS Server Information from Clients

When the Digi router is using DHCP to assign LAN device IP addresses, it will normally pass the carrier supplied DNS server IP addresses to clients. It may be desirable to block the carrier DNS server IP addresses from passing. Today, this must be done via the command line. The syntax is:

```
set ppp port=n ipcp_dns_enabled=off
```

"n" is the PPP port being used by the mobile interface. For a ConnectPort WAN this will be 5; for other Digi cellular routers it will usually be "2". Enter "set ppp" with no parameters to view the enabled PPP ports.

Static DNS servers can be entered into the Digi device's network configuration screen. The DNS priority can be changed in the Network > Advanced Settings screen.

## 3 Wireless LAN (802.11) Security

Some ConnectPort gateway modules can accept an optional 802.11 Wireless LAN adapter. This adapter works in Ad-Hoc (peer-to-peer) mode only and is therefore not a wireless access point.

Wireless authentication and encryption mechanisms are supported via WAP, WEP, LEAP, TKIP and 802.x protocols.

Refer to the WebUI Configuration > Wi-Fi Security or "set wlan" CLI commands for details.

## 4 Cellular Carrier and RF Security

### 4.1 IP Addressing and Secure Connectivity Options

Work with your carrier to obtain a plan that meets your security needs and your budget. The wireless carrier may offer plans that greatly enhance security. Check with your carrier to see what options they offer. Here are three carrier-related options that can help with securing data traffic and access to the Digi gateway:

1. Use a plan that blocks some or all traffic into the Digi gateway from the mobile network. For example, some carriers have plans which allow only remote initiated traffic; internal firewalls will block any unsolicited inbound traffic. However, this type plan cannot be used if your application requires you to reach out to the remote site to for example poll a meter (some carriers call this mobile terminated data). Other carriers have plans that may block

only certain traffic such as HTTP on TCP port 80 or pings, or use “restricted IP addresses” where that even though they use public IP addresses, access is restricted internally by the carrier.

2. Use a completely private plan. Here, the carrier may be able to supply a direct connection into your network via Frame Relay, MPLS or IPsec VPN. In many cases, private IP addresses can be assigned to the Digi gateway’s mobile interface and controlled by you, the customer; and the data never touches the Internet.
3. Use dynamic mobile IP addresses but not use Dynamic DNS. This, however, will likely restrict your application to only outbound initiated connections.

## 4.2 RF and Modem Security

### 4.2.1 How the Device is Identified and Authenticated

Depending on the wireless technology used (meaning GSM vs. CDMA) and the carrier, there are several ways the Digi gateway cellular device is identified and authenticated on the cellular network.

GSM devices use a SIM (Subscriber Identity Module) which is typically the first level of identification to the network. The modem’s IMEI (International Mobile Equipment Identity, i.e., the modem serial number) can in some cases be used to identify the device. Other information such as plan/APN name, username and password may also be required, and are configured in the mobile settings of the Digi device.

CDMA devices in the U.S. do not use a SIM*, instead they are identified on the network by the modem’s electronic serial number, the ESN. Some carriers use only the ESN for authentication, while others may require additional information such as a service programming code (SPC/MSL), user-name, and password be entered into the Digi device’s configuration.

(* CDMA devices in China and other locations may require a SIM. Digi does not support SIMs in CDMA devices as of this writing.)

### 4.2.2 Over the Air (OTA) Security

The link between the embedded modem and the cellular base station (tower) and possibly farther into the wireless carrier network is encrypted. Different carriers and technologies will use various types and levels of encryption, typically either 64-bit or 128-bit. Frequency and code hopping also make it virtually impossible to eavesdrop on a cellular connection.

Check with your carrier for specifics on what security mechanisms they employ.

# 4. A Note on PCI Compliance

Payment Card Industry Data Security Standards (PCI DSS) are requirements for payment card security used in point of sale, retail and banking applications. As of this writing there are no specific PCI certifications for network devices. Instead, PCI compliance is for an entire system, not just a single network component.

A device can be considered part of a “PCI compliant” system if it (a) does not store credit card information, (b) does not make data traffic available via trace mechanisms, and (c) can be secured so that unauthorized access cannot be used to redirect transactions.

Digi cellular gateways can be deployed as part of a PCI-compliant solution because they:

- Support IPsec and SSL tunneling using 3DES or up-to-256-bit AES encryption. Both pre-shared keys and X.509 digital certificates are supported for authentication.
- Include IP Filtering and NAT to limit access to the device from specific network(s) and/or IP host(s); as well as the ability to disable/change IP services.
- Provide username / password authentication to secure access to the device thus limiting who can make changes.
- Do not store cardholder information nor provide a mechanism to capture/trace data traffic.

Finally, as stated above, check with your carrier on how their network can provide additional security such as private plans that do not access the Internet.

---

To learn more about Digi's family of cellular gateways, visit:
www.digi.com/products/cellulargateways/

To learn more about Drop-in Networking, visit:
www.digi.com/products/wirelessdropinnetworking/

Please call 952-912-3444 or email info@digi.com for more information.

2008-05-14