Digi Connect® Family User's Guide

Digi Connect Family Products:
Digi Connect SP, Digi Connect Wi-SP, Digi Connect ME, Digi Connect ME4,
Digi Connect Wi-ME, Digi Connect EM, Digi Connect Wi-EM,
Digi Connect ES (Digi Connect ES 4/8/16 devices)

Digi ConnectPort™ Products:
ConnectPort TS 8
ConnectPort TS 8 MEI

90000565_H

Contents

About this Guide

Purpose

This guide describes and shows how to configure, monitor, and administer Digi Connect Family products.

Audience

This guide is intended for those responsible for setting up Digi Connect Family products. It assumes some familiarity with networking concepts and protocols. A glossary is provided with definitions for networking terms and features discussed in the content.

Scope

This guide focuses on configuration, monitoring, and administration of Digi Connect Family products. It does not cover hardware details beyond a certain level, application development, or customization of Digi Connect Family products.

Where to Find More Information

In addition to this guide, find additional product and feature information in the these documents:

General Release Documentation

These documents are of interest to end users of Digi Connect Family devices:

- Online help and tutorials
- Context-sensitive assistance available in the Web-based interface to Digi Connect Family devices.
- Digi Connect Hardware Reference Guides
- Digi Connect ES Device Server Hardware Setup Guide
- Quick Start Guides
- RealPort® Installation Guide
- Digi Connect Family Customization and Integration Guide
- Connectware Manager Getting Started Guide and Operator's Guide
- Release Notes
- Cabling Guides

Integration Documentation

For customers who purchase the Digi Connect Integration Kit for product customization, the Integration Kit includes such resources as development board schematics for module products, firmware release notes, hardware reference manuals, specifications, and documentation for the sample applications. For more information, see the document *Getting Started with Digi Connect* included with the Integration Kit and accessed from the Start menu (**Start > Digi Connect > Getting Started with Digi Connect**).

Additional Product Information on www.digi.com

In addition to the previous documents, product information is available on the Digi website, **www.digi.com**, including:

- Support Forums
- Knowledge Base
- Data sheets/product briefs
- Application/solution guides

Digi Contact Information

For more information about Digi products, or for customer service and technical support, contact Digi International.

To Contact Digi International by:	Use:
Mail	Digi International 11001 Bren Road East Minnetonka, MN 55343 U.S.A.
World Wide Web:	http://www.digi.com/support/
email	http://www.digi.com/support/
Telephone (U.S.)	(952) 912-3444 or (877) 912-3444
Telephone (other locations)	+1 (952) 912-3444 or (877) 912-3444

Introduction

CHAPTER 1

This chapter introduces the products in the Digi Connect Family, features, types of connections and data paths in which Digi Connect products can be used, and the interface options available for configuring, monitoring, and administering Digi Connect Family products.

The Digi Connect Family

Digi Connect Family products include:

Digi Connect SP™

The Digi Connect SP (Single Port) device server is the ideal platform for custom web- and network-enabled embedded applications. Combining Digi and NetSilicon technology, it eliminates the hardware design effort and delivers a true device networking solution that is powerful enough to meet future performance requirements.

Built on leading NetSilicon 32-bit NET+ARM technology, the Digi Connect SP device server provides a powerful off-the-shelf hardware platform for embedded web- and network applications with a seamless migration path to embedded modules and a fully integrated NetSilicon system-on-chip solution using the award-winning family of Ethernet-enabled NET+ARM microprocessors.

Digi Connect Wi-SP™

The Digi Connect Wi-SP (Wireless Single Port) device server is a secure 802.11b wireless network solution. Combining Digi and NetSilicon technology, configuration is simple without complex integration tools. The compact hardware design delivers a powerful networking solution to meet performance requirements.

Built on leading NetSilicon 32-bit NET+ARM technology, the Digi Connect Wi-SP device server provides a powerful off-the-shelf hardware platform for embedded web- and network applications with a seamless migration path to embedded modules and a fully integrated NetSilicon system-on-chip solution using the award-winning family of Ethernet-enabled NET+ARM microprocessors.

Digi Connect ME™

The Digi Connect ME (Micro Embedded) device server enables manufacturers to keep pace with ever-evolving networking technology by easily adding web-enabled network connectivity to existing products. This network connectivity is provided without the added complexities of extensive hardware and software integration, and at a fraction of the time and cost that would be required to develop a custom solution.

Built on leading 32-bit ARM technology using the network-attached NetSilicon NS7520 microprocessor, the Digi Connect ME combines true plug-and-play functionality with the freedom and flexibility of complete product customization options. These options are based on the NetSilicon NET+Works development platform. This platform offers a seamless migration path to a fully integrated NetSilicon system-on-chip solution.

The Digi Connect ME Integration Kit is available to help customize the look-and-feel of the device interface.

Digi Connect Wi-ME™

The Digi Connect Wi-ME (Wireless Micro Embedded) is a fully customizable and secure 802.11b wireless device server. It is based on the common platform design approach of the Digi Connect family of embedded products, which minimizes design risk and reduces time to market by allowing customers to easily accommodate both wired and wireless network functionality in a single future-proof product design.

The Digi Connect Wi-ME device server is pin-compatible with the Digi Connect ME, and makes fully transparent 802.11b integration possible without the traditional complexities of hardware and software integration work.

Built on leading NetSilicon 32-bit NET+ARM technology, the Digi Connect Wi-ME embedded module offers a seamless migration path to a fully integrated NetSilicon system-on-chip solution. It combines true plug-and-play functionality with the freedom and flexibility of complete software customization using the proven NetSilicon NET+Works development platform.

The Digi Connect Wi-ME Integration Kit is available to help customize the look-and-feel of the device interface.

Digi Connect EM™

The Digi Connect EM (Embedded Module) device server delivers true Web-enabled device networking that is easy and cost-effective to implement, while being powerful enough to meet future performance needs.

Built on leading 32-bit ARM technology using the network-attached NetSilicon NS7520 microprocessor and featuring a wide variety of connectivity options, the Digi Connect EM provides the freedom and flexibility of complete custom product development.

The Digi Connect EM Integration Kit is available to help customize the look-and-feel of the device interface.

Digi Connect Wi-EM™

The Digi Connect Wi-EM (Wireless Embedded Module) device server is a fully customizable and secure 802.11b wireless embedded module that provides integration flexibility in a variety of connection options. Based on the common platform design approach of the Digi Connect family of embedded products, the Digi Connect Wi-EM minimizes design risk and reduces time to market by allowing customers to easily accommodate both wired and wireless network functionality in a single future-proof product design.

The Digi Connect Wi-EM wireless embedded module is pin-compatible with the Digi Connect EM, and makes fully transparent 802.11b integration possible without the traditional complexities of hardware and software integration work.

Built on leading NetSilicon 32-bit NET+ARM technology, the Digi Connect Wi-EM combines true plug-and-play functionality with the freedom and flexibility of complete software customization using the proven NetSilicon NET+Works development platform, and offers a seamless migration path to a fully integrated NetSilicon system-on-chip solution.

The Digi Connect Wi-EM Integration Kit is available to help customize the look-and-feel of the device interface.

Digi Connect™ ES

The Digi Connect ES (Extended Safety) provides sensitive serial over Ethernet connectivity for applications. It is the first IEC 60601/EN60601 compliant device of its kind and consists of four, eight, or 16 galvanically isolated RS-232 serial ports, with a 10/100 Mbps network interface and Ethernet switch (eight- 16-port models). Common applications include providing Ethernet connections from serial devices such as ventilators, EKGs, patient monitoring systems, infusion pumps and glucose meters to the central data management system.

Galvanical isolation provides extended electrical safety. There is no electrical path for current to earth ground, ensuring no electrical shock when making physical contact with the Digi Connect ES. There is no electrical path from port to port, ensuring a ground fault will not affect the operation of the Digi Connect ES for the operation of any device connected to it.

Digi ConnectPort™ TS Products

Digi ConnectPort TS (Terminal Server) products provide serial over Ethernet connectivity for applications today and into the future. They support IPv4 and IPv6 Ethernet protocols. The Digi ConnectPort TS 8 MEI product is the same size as the Digi ConnectPort TS 8 (RS-232 only) and is the smallest 8-port device with a Multiple Electrical Interface (MEI) in the industry.

Features

This is an overview of key features in Digi Connect Family products. Software features are covered in more detail in the next three chapters. Hardware specifications and are covered in Chapter 5, "Specifications and Certifications".

User Interfaces

There are several user interfaces for configuring and monitoring Digi Connect Family products, including:

- The Digi Device Setup Wizard, a wizard-based tool for assigning an IP address to a Digi Connect device, minimally configuring it, and installing RealPort software on a PC or server.
- A Web-based interface for configuring, monitoring, and administering Digi Connect devices.
- An optional Java-applet interface.
- A command-line interface.
- Configuration through Remote Command Interface (RCI) over the serial port.
- Simple Network Management Protocol (SNMP).
- The Connectware Manager Console.

For additional details on these user interfaces, see "Configuration Interfaces" on page 44 and "Monitoring Interfaces" on page 59. Some user interfaces can be customized.

Quick Reference for Configuring Features

This guide primarily focuses on configuring, monitoring, and administering Digi products from the Web user interface. This table provides a quick reference for configuring features and performing device tasks, and where to find the features and settings in the Web user interface and this guide. Click the page number in the Page column to jump to instructions on configuring or using the feature. Some features are configurable from the command line interface only. In those cases, the commands that configure the feature are noted. The command descriptions are in the *Digi Connect Family Command Reference*.

Feature/Task	Path to Feature in the Web User Interface	See Page
Administration/Configuration management:		
■ File management: uploading and downloading files, such as applet files, and custom splash screens.	**Administration > File Management** See also the *Digi Connect Family Customization and Integration Guide* for information on uploading and downloading files used to customized a Digi device's look-and-feel.	157
■ Backup/restore a configuration from a TFTP server on the network	**Administration > Backup/Restore**	158
■ Update firmware	**Administration > Update Firmware**	159
■ Reset configuration to factory defaults	**Administration > Factory Default Settings**	160
■ System information, including device identifiers and statistics	**Administration > System Information**	163
■ Reboot the Digi device	**Administration > Reboot**	163
Alarms	**Configuration > Alarms**	104
Autoconnection: automatically connect a user to a server or network device	**Configuration > Serial Ports > *port* > Profile Settings > TCP Sockets > Automatically establish TCP connections**	93

Feature/Task	Path to Feature in the Web User Interface	See Page
Connection management:		
■ Manage serial port connections	**Management > Serial Ports**	149
■ Manage active system connections	**Management > Connections > Active System Connections**	149
Domain Name System (DNS):		
■ DNS Client	**Configuration > Network > IP Settings > Primary DNS** and **Secondary DNS**	79
Ethernet settings	**Configuration > Network > Advanced Network Settings**	90
General Purpose Input/Output (GPIO) pins	**Configuration > GPIO**	100
Help on configuring features	**Help** button on each page.	
Host name for a device	**Configuration > Network > Advanced Network Settings > Host Name**	90
IP address settings:		
■ Using static IP addresses	**Configuration > Network > IP Settings**	64, 79
■ Using DHCP	**Configuration > Network > IP Settings**	65, 79,
■ Using Auto IP	**Configuration > Network > Advanced Settings**	65, 90
Modem emulation	**Configuration > Serial Ports > Port Profile Settings > Modem Emulation** See the *Connect Family Command Reference* for modem emulation commands.	95
Multiple Electrical Interface (MEI)	Currently available in ConnectPort TS models only, and configurable from command line only. See the **set switches** command in the *Connect Family Command Reference*.	

Feature/Task	Path to Feature in the Web User Interface	See Page
Port logging: enabling port buffering and displaying contents of a port buffer	To enable port logging: **Configuration > Serial Ports > Advanced Serial Settings** To display the contents of a port buffer: **Management > Serial Ports > Port Logs**	97
Port profiles: sets of preconfigured serial-port settings for a particular connection and use scenario	**Configuration > Serial Ports > Port Profile Settings**	91
Remote Command Interface (RCI) as a device interface	N/A	56
RealPort (COM port redirection) configuration	**Configuration > Serial Ports > *port* > Port Profile Settings > RealPort** See also the *RealPort Installation Guide*.	92
Reverting configuration settings	**Administration > Factory Default Settings**	160
Security/access control features:		
■ Control access to inbound ports	**Configuration > Serial Ports > *port* > Port Profile Settings > TCP Sockets** or **UDP Sockets** or **Custom port profile**	91
■ Enable/disable command-line access	**Configuration > Serial Ports > *port* > Port Profile Settings > Local Configuration > Access the command line interface when connecting from serial terminals** or **Configuration > Serial Ports > *port* > Port Profile Settings > Custom > Access the command line interface**	95
■ Secure Shell Server (SSH)	**Network > Network Services > Enable Secure Shell Server (SSH)**	87
■ Establish/change user name for a user	**Configuration > Users >** select a user to change**,** or select **Add New User** for a new user	114
■ Issue a new/changed password to a user	**Configuration > Users >** select a user to change or select **Add New User for a new user**	114

Feature/Task	Path to Feature in the Web User Interface	See Page
■ Set permissions associated with various services and commands	**Configuration > Users >** select a user to change or add	118
Serial port configuration:		
■ Basic serial port settings	**Configuration > Serial Ports > Basic Serial Settings**	96
■ Advanced serial port settings	**Configuration > Serial Ports > Advanced Serial Settings**	97
■ Port profiles: associate a serial port with a set of preconfigured port settings for a specific use	**Configuration > Serial Ports > Port Profile Settings**	91
■ RCI over serial mode	**Configuration > Serial Ports > Advanced Serial Settings**	97
■ RTS Toggle	**Configuration > Serial Ports > Advanced Serial Settings**	97
■ TCP serial connections	**Configuration > Serial Ports > *port* > Port Profile Settings > TCP Sockets port profile**	93
■ UDP serial characteristics	**Configuration > Serial Ports > *port* > Port Profile Settings > UDP Sockets port profile**	94
Simple Network Management Protocol (SNMP):		
■ Configure SNMP through the Web user interface	**Configuration > System > Simple Network Management Protocol (SNMP) Settings**	108
■ Enable/disable SNMP service	**Configuration > Network > Network Services**	84
■ Enable/disable SNMP alarm traps	**Configuration > Alarms > *alarm* > Send SNMP trap to following destination when alarm occurs**	106, 107

Feature/Task	Path to Feature in the Web User Interface	See Page
■ Use SNMP as primary configuration interface	Basic network and serial settings configurable through standard and Digi-specific Management Information Blocks (MIBs). More advanced settings must be set through the Web or command-line user interfaces, and sending alarms as SNMP traps must be configured through the Web user interface, on the pages listed above.	57, 137
System information: assign system-identifying information to a device	**Configuration > System > Device Identity Settings**	108
Statistics for Digi devices	**Administration > System Information**	140
Status of Digi devices	**Management > Serial Ports, Connections, Network Services**	
Wireless devices:		
Wireless LAN Settings	**Configuration > Network > Wireless LAN Settings**	79
Wireless Security Settings	**Configuration > Network > Wireless Security Settings**	81
Wireless 802.1x Authentication Settings	**Configuration > Network > Wireless 802.1x Settings**	83
Ekahau Client™ device-location software	**Applications > Ekahau Client**	121

Hardware Features

A summary of hardware features, including power-supply information, is in "Hardware Specifications" on page 169. For detailed hardware specifications, see the *Hardware Reference* and data sheet for your Digi Connect product.

Network Interface Features

A detailed list of network interface features is in Chapter 5, "Specifications and Certifications". See also the data sheet for your Digi product.

Configurable Network Services

Access to network services can be enabled and disabled. This means that a device's use of network services can be restricted to those strictly needed by the device. To improve device security, non-secure services, such as Telnet, can be disabled.

Network services that can be enabled or disabled include:

- Advanced Digi Discovery Protocol (ADDP): can enable or disable ADDP, but cannot change its network port number.
- RealPort
- Encrypted RealPort
- HTTP/HTTPS
- Line Printer Daemon (LPD)
- Remote Login (rlogin)
- Remote Shell (rsh)
- Simple Network Management Protocol (SNMP)
- Telnet

In the Web user interface, access to network services is enabled and disabled on the Network Services page of Network Configuration. For more information, see "Network Services Settings" on page 84. In the command-line interface, network services are enabled and disabled through the **set service** command. See the *Digi Connect Family Command Reference* for the **set service** command description.

IP Protocol Support

All the products in the Digi Connect Family include a Robust on-board TCP/IP stack with a built-in web server. The protocols supported in each Digi Connect Family include, unless otherwise noted:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Dynamic Host Configuration Protocol (DHCP)
- Simple Network Management Protocol (SNMP)
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
- Telnet Com Port Control Option (Telnet) including support of RFC 2217 (ability to control serial port through Telnet).See "Serial Data Communication over TCP and UDP" on page 30 for additional information.
- Remote Login (rlogin)
- Line Printer Daemon (LPD)
- HyperText Transfer Protocol (HTTP)/HyperText Transfer Protocol over Secure Socket Layer (HTTPS)
- Simple Mail Transfer Protocol (SMTP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- Address Resolution Protocol (ARP)
- Advanced Digi Discovery Protocol (ADDP)
- Network Address Translation (NAT)/Port Forwarding

Following is an overview of some of the services provided by these protocols.

Serial Data Communication over TCP and UDP

Digi Connect Familysupport serial data communication over TCP and UDP.Key features include:

- Serial data communication over TCP, also known as autoconnect and tcpserial can automatically perform the following functions:
  - Establish bidirectional TCP connections, known as autoconnections, between the serial device and a server or other network device. Autoconnections can be made based on data and or serial hardware signals.
  - Control forwarding characteristics based on size, time, and pattern
  - Allow incoming raw, Telnet, and SSL/TLS (secure-socket) connections
  - Support RFC 2217,
- Serial data communication over UDP, also known as udpserial, can automatically perform the following functions:
  - Digi Connect products can automatically send serial data to one or more devices or systems on the network using UDP sockets. Options for sending data include whether specific data is on the serial line, a specific time period has elapsed, or after the specified number of bytes has been received on the serial port.
  - Control forwarding characteristics based on size, time, and patterns.
  - Support incoming datagrams from multiple destinations.
  - Support outgoing datagrams sent to multiple destinations.
- TCP/UDP forwarding characteristics.
- Extended communication control on TCP/UDP data paths.
  - Timeout
  - Hangup
  - User-configurable Socket ID string (text string identifier on autoconnect only)

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) can be used to automatically assign IP addresses, deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and provide other configuration information. For further details, see "IP Address Assignment" on page 34.

Auto-IP

Auto-IP is a protocol that will automatically assign an IP address from a reserved pool of standard Auto-IP addresses to the computer on which it is installed. Digi devices are set to obtain its IP address automatically from a DHCP server. But if the DHCP server is unavailable or nonexistent, Auto-IP will assign the device an IP address. For further details, see "IP Address Assignment" on page 34.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a protocol for managing and monitoring network devices. SNMP architecture enables a network administrator to manage nodes--servers, workstations, routers, switches, hubs, etc.--on an IP network; manage network performance, find and solve network problems, and plan for network growth. Digi Connect Family products support SNMP Version 1. For more information on SNMP as a device-management interface, see "Simple Network Management Protocol (SNMP)" on page 57.

Supported RFCs and MIBs

Digi Connect Family products support these SNMP-related Request for Comments (RFCs) and Management Information Bases (MIBs):

- RFC 1213 - Management Information Base (MIB) II
- RFC 1215 - Generic Traps (coldStart, linkUp, authenticationFailure only)
- RFC 1316 - Character MIB
- RFC 1317 - RS-232 MIB
- DIGI-DEVICE-INFO.mib - A Digi enterprise MIB for the Digi Connect Family.
- DIGI-SERIAL-ALARM-TRAPS.mib - A Digi enterprise MIB for sending alarms as SNMP traps.

Supported SNMP Traps

SNMP traps can be enabled or disabled. Supported SNMP traps include:

- Authentication failure
- Login
- Cold start
- Link up
- Alarms can be issued in the form of SNMP traps

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) are used to provide authentication and encryption for Digi Connect Family products. For more information, see "Security Features" on page 37.

Telnet

Digi Connect Family products support the following types of Telnet connections:

- Telnet Client
- Telnet Server
- Reverse Telnet, often used for console management or device management
- Telnet Autoconnect
- RFC 2217, Telnet Com Port Control Option, an extension of the Telnet protocol

For more information on these connections, see "Supported Connections and Data Paths" on page 40. Access to Telnet network services can be enabled or disabled.

Remote Login (rlogin)

Users can perform logins to remote systems (rlogin). Access to rlogin service can be enabled or disabled.

Line Printer Daemon (LPD)

The Line Printer Daemon (LPD) allows network printing over a serial port.Each serial port has a dedicated LPD server that is independently configurable. Access to LPD service can be enabled or disabled.

HyperText Transfer Protocol (HTTP)
HyperText Transfer Protocol over Secure Socket Layer (HTTPS)

Digi Connect products provide web pages for configuration that can be secured by requiring a user login.

Internet Control Message Protocol (ICMP)

ICMP statistics can be displayed, including the number of messages received, bad messages received, and destination unreachable messages received.

Point-to-Point Protocol (PPP)

The Point-to-Point Protocol (PPP) transports multi-protocol packets over point-to-point links. PPP encapsulates the data packet, allows the server to inform the dial-up client of its IP address (or client to request the IP address), authenticates the exchange, negotiates multiple protocols, and reassembles the data packet for network communication.

Network Address Translation (NAT)/Port Forwarding

NAT) reduces the need for a large amount of publicly known IP addresses by creating a separation between publicly known and privately known IP addresses.

Advanced Digi Discovery Protocol (ADDP)

The Advanced Digi Discovery Protocol (ADDP) runs on any operating system capable of sending multicast IP packets on a network. ADDP allows the system to identify all ADDP-enabled Digi devices attached to a network by sending out a multicast packet. The Digi devices respond to the multicast packet and identify themselves to the client sending the multicast.

ADDP needs to communicate with the TCP/IP stack using UDP. The TCP/IP stack should be able to receive multicast packets and transmit datagrams on a network.

Not all Digi devices support ADDP.

Access to ADDP service can be enabled or disabled, but the network port number for ADDP cannot be changed from its default.

IP Address Assignment

There are several ways to assign an IP address to a Digi Connect Familyproduct:

- Static IP: Assign a specific IP address to a device, through the Digi Device Setup Wizard, the Web user interface, or the command-line interface.
- Using Dynamic Host Configuration Protocol (DHCP). Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information. All Digi Connect Family devices except Digi Connect WAN IA have a DHCP server enabled by default. Digi Connect WAN IA is configured by default to be a DHCP client.
- Auto Private IP Addressing (APIPA), also known as Auto-IP: A standard protocol that will automatically assign an IP address from a reserved pool of standard Auto-IP addresses to the computer on which it is installed. The device is set to obtain its IP address automatically from a DHCP server. But if the DHCP server is unavailable or nonexistent, Auto-IP will assign the device an IP address. If DHCP is enabled or responds later ADDP is used, both will override the Auto-IP address previously assigned.

For more details, see "Alternate Methods for Assigning an IP Address" on page 64.

RealPort Software

Digi Connect Family products use the patented RealPort COM/TTY port redirection for Microsoft Windows, UNIX, and Linux environments. RealPort software provides a virtual connection to serial devices, no matter where they reside on the network. The software is installed directly on the host PC and allows applications to talk to devices across a network as though the devices were directly attached to the host. Actually, the devices are connected to a Digi device somewhere on the network.

RealPort is unique among COM port re-directors because it is the only implementation that allows multiple connections to multiple ports over a single TCP/IP connection. Other implementations require a separate TCP/IP connection for each serial port. Unique features also include full hardware and software flow control, as well as tunable latency and throughput.

Access to RealPort services can be enabled or disabled.

Encrypted RealPort

Digi Connect Family products support the patent-pending RealPort software with encryption.Encrypted RealPort offers a secure Ethernet connection between the COM or TTY port and a device server or terminal server. Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in a Secure Sockets Layer (SSL) connection and encrypting the data using Advanced Encryption Standard (AES), one of the latest, most efficient security algorithms. Access to Encrypted RealPort services can be enabled or disabled.

Digi's RealPort with encryption driver has earned Microsoft's Windows Hardware Quality Lab (WHQL) certification.

Drivers are available for a wide range of operating systems, including Microsoft Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows 98, Windows ME; SCO Open Server; Linux; AIX; Sun Solaris SPARC; Intel; and HP-UX. It is ideal for financial, retail/point-of-sale, government or any application requiring enhanced security to protect sensitive information.

Alarms

Digi Connect Family products can be configured to issue alarms, in the form of email message or SNMP traps, when certain device events occur. These events include changes in GPIO signals, certain data patterns being detected in the data stream. Receiving alarms about these conditions provides the advantage of notifications being issued when events occur, rather than having to monitor the device on an ongoing basis to determine whether these events have occurred. For more information on configuring alarms, see "Configure Alarms" on page 104.

Modem Emulation

Digi Connect Family products include a configuration profile that allows the device to emulate a modem. Modem emulation sends and receives modem responses to a serial device over TCP/IP (including Ethernet) instead of Public Switched Telephone Network (PSTN). The modem emulation profile allows maintaining a current software application but using it over the less expensive Ethernet network. In addition, Telnet processing can be enabled or disabled on the incoming and outgoing modem-emulation connections.The modem-emulation commands supported in Digi Connect devices are documented in the *Digi Connect Family Command Reference*.

Security Features

Security-related features in Digi Connect Family products include:

- Secure access and authentication:
  - One password, one permission level.
  - Can issue passwords to device users.
  - 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.
  - Can control access to specific devices, IP addresses, or networks through IP filtering.
  - User and user group access permissions, which control user access to various features and the level of control they have over them (view settings or change settings).
- Encryption:
  - Strong Secure Sockets Layer (SSL) V3.0/ Transport Layer Security (TLS) V1.0-based encryption: DES (58-bit), 3DES (168-bit), AES (128-/156-bit), IPsec ESP: DES, 3DES, AES.
  - Strong Secure Sockets Layer (SSL) V3.0/ Transport Layer Security (TLS) V1.0-based encryption: DES (64-bit), 3DES (192-bit), AES (128-/192-/256-bit), IPsec ESP: DES, 3DES, AES.
  - Encrypted RealPort offers encryption for the Ethernet connection between the COM/TTY port and the Digi Connect Family device.
  - Wireless Digi Connect products provide Wi-Fi Protected Access (WPA/WPA2/802.11i) and Wired Equivalent Privacy (WEP) encryption (64-/128-bit). Supported WPA/WPA2/802.11i authentication methods are:

Supported WPA Authentication Methods		
EAP-TLS	**PEAP**	**EAP/TTLS**
LEAP (WEP only)	EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-MD5-Challenge
	EAP-PEAP/TLS (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-GTC
	EAP-PEAP/GTC (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-OTP
	EAP-PEAP/OTP (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-MSCHAPv2
	EAP-PEAP/MD5-Challenge (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-TLS
		EAP-TTLS/MSCHAPv2
		EAP-TTLS/MSCHAP
		EAP-TTLS/PAP
		EAP-TTLS/CHAP

- 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.

Configuration Management

Once a Digi Connect Family product is configured and running, configuration-management tasks need to be periodically performed, such as:

- Upgrading firmware
- Copying configurations to and from a remote host
- Software and factory resets
- Rebooting the device
- Memory management
- File management

For more information on these configuration-management tasks, see Chapter 4, "Administration Tasks".

Customization Capabilities

Several aspects of using Digi Connect Family products can be customized. For example:

- The look-and-feel of the device interface can be customized, to use a different company logo or screen colors.
- Custom Java applets can be created, using the Java configuration applet as a sample for further development.
- Custom factory defaults to which devices can be reverted can be defined.

The *Digi Connect Family Customization and Integration Guide* (Part Number 90000734; available with the Digi Connect Integration Kit) describes customization and integration tools and processes. Contact Digi International for more information onthe Digi Connect Integration Kit customization tools and resources and for assistance with customization efforts.

The Digi Connect Integration Kit provides a platform for evaluation, rapid prototyping, and integration of Digi Connect embedded modules with plug-and-play firmware. It includes tools, sample code, and documentation to help with product integration and web-based customization efforts.

Supported Connections and Data Paths

Digi Connect Family products allow for several kinds of connections and paths for data flow between the Digi device and other entities. These connections can be grouped into two main categories:

- Network services, in which a remote entity initiates a connection to a Digi device.
- Network/serial clients, in which a Digi device initiates a network connection or opens a serial port for communication.

Following is a discussion of these connections. The intent of this information is to illustrate how the connections are made and data is passed. This in turn may help understand the effects of enabling certain features and choosing certain settings when configuring Digi products.

Network Services

A network service connection is one in which a remote entity initiates a connection to a Digi device. There are several categories of network services:

- Network services associated with specific serial ports
- Network services associated with serial ports in general
- Network services associated with the command-line interface (CLI)

Network Services Associated with Specific Serial Ports

Network service connections associated with specific serial ports include:

- Reverse Telnet: A telnet connection is made to a Digi device, in which data is passed transparently between the telnet connection and a named serial port.
- Reverse raw socket: A raw TCP socket connection is made to a Digi device, in which data is passed transparently between the socket and a named serial port.
- Reverse TLS socket: An encrypted raw TCP socket is made to a Digi device, in which data is passed transparently to and from a named serial port.
- LPD: A TCP connection is made to a named serial port, in which the Digi device interprets the LPD protocol and sends a print job out of the serial port.

- Modem emulation, also known as Pseudo-modem (pmodem): A TCP connection is made to a named serial port, and the connection will be "interpreted" as an incoming call to the pseudo-modem.

Network Services Associated with Serial Ports in General

Network service connections associated with serial ports in general include

- RealPort: A single TCP connection manages (potentially) multiple serial ports.
- Modem emulation, also known as pseudo-modem (pool): A TCP connection to the "pool" port is interpreted as an incoming call to an available pseudo-modem in the "pool" of available port numbers.
- rsh: Digi products support a limited implementation of the Remote shell (rsh) protocol, in that a single service listens to connections and allows a command to be executed. Only one class of commands is allowed: a single integer that specifies which serial port to connect to. Otherwise, the resulting connection is somewhat similar to a reverse telnet or reverse socket connection.

Network Services Associated with the Command-Line Interface

Network service connections associated with the command-line interface include:

- Telnet: A user can Telnet directly to a Digi device's command-line interface.
- rlogin: A user can perform a remote login (rlogin) to a Digi device's command-line interface.

Network/Serial Clients

A network/serial client connection is one in which a Digi device initiates a network connection or opens a serial port for communication. There are several categories of network/serial client connections:

- Autoconnect behavior client connections
- Command-line interface (CLI)-based clients
- Modem emulation (pseudo-modem) client connections

Autoconnect Behavior Client Connections

In client connections that involve autoconnect behaviors, a Digi device initiates a network connection based on timing, serial activity, or serial modem signals. Autoconnect-related client connections include:

- Raw TCP connection: The Digi device initiates a raw TCP socket connection to a remote entity.
- Telnet connection: The Digi device initiates a TCP connection using the Telnet protocol to a remote entity.
- Raw TLS encrypted connection: The Digi device initiates an encrypted raw TCP socket connection to a remote entity.
- Rlogin connection: The Digi device initiates a TCP connection using the rlogin protocol to a remote entity.

Command-Line Interface (CLI)-based Client Connections

Command-line interface based client connections are available for use once a user has established a session with the Digi Connect device's CLI. CLI-based client connections include:

- telnet: A connection is made to a remote entity using the Telnet protocol.
- rlogin: A connection is made to a remote entity using the Rlogin protocol.
- connect: Begin communicating with a local serial port.

Modem Emulation (Pseudo-Modem) Client Connections

When a port is in the modem-emulation or pseudo-modem mode, it can initiate network connections based on AT command strings received on the serial port.The AT commands for modem emulation are documented in the *Digi Connect Family Command Reference*.

Configuration Capabilities and Interfaces

Following is an overview of the configuration capabilities and interfaces for Digi Connect Family products. Chapter 2, "Configure Digi Connect Family Devices" covers these capabilities and interfaces in more detail.

Configuration Capabilities

Device configuration involves setting values and enabling features for such areas as:

- Network configuration: Specifying the device's IP address and IP settings, network-service settings, and advanced network settings.
- Serial port configuration: Specifying the serial port characteristics for the device.
- GPIO pin configuration (for all devices except Digi Connect SP, Digi Connect Wi-SP): Specifying how the various GPIO pins for the device will be used.
- Alarms: Defining whether alarms should be issued, the conditions that trigger alarms, and how the alarms should be delivered.
- Security/Users configuration: Configuring security features, such as whether password authentication is required for device users.
- System configuration: Specifying system-identifying information, such as a device description, contact person, and physical location.

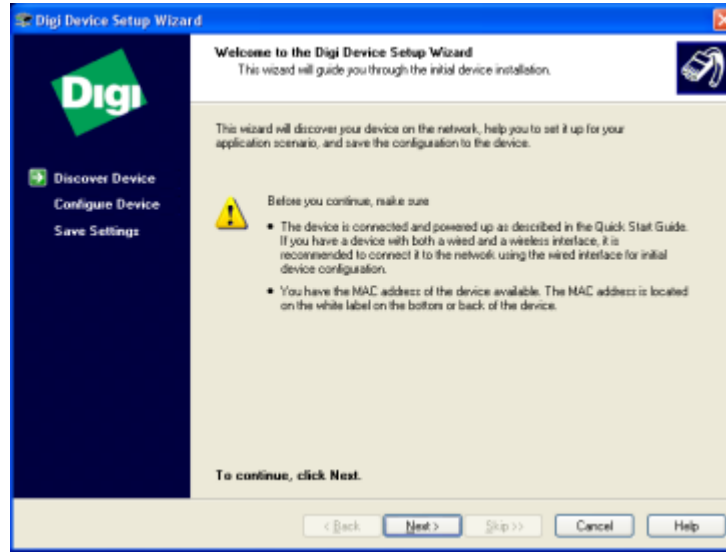
Configuration Interfaces

Several interfaces are available for configuring Digi Connect Family products, including:

- The Digi Device Setup Wizard, which helps set up an IP address for the device and quickly configure features.
- The Digi Device Discovery Utility, which locates Digi devices on a network, and allows opening the Web user interface for the devices.
- A Web-based interface embedded with the product, providing device configuration profiles for quick serial-port configuration and other settings.
- An optional Java applet that can be used for device configuration, and as a sample application for customization and further application development.
- A command-line interface (CLI).
- Connectware Manager, a configuration interface to fine-tune or monitor Connectware devices. Connectware Manager cannot assign an IP address but it can change one.
- Remote Command-line Interface (RCI) protocol.
- Simple Network Management Protocol (SNMP).

The Digi Device Setup Wizard

The Digi Device Setup Wizard is a wizard, for configuring Digi Connect Family products. It is provided on the CD shipped with each product. Using the Digi Device Setup Wizard is the recommended and preferred method for configuration. It assigns an IP address for the device, configures the device's serial port parameters based on a selected configuration scenario called a port profile, and determines whether RealPort software needs to be installed.



Using the Digi Device Setup Wizard provides these advantages:

- The Digi Device Setup Wizard is the preferred approach for initial configuration. For most users, the Digi Device Setup Wizard interface provides adequate device configuration.
- Device configuration is made easier by providing a set of port profiles which configure a serial port based on the way the port will be used. Each port profile displays the relevant settings for the configuration. There are several profile choices, including RealPort, Console Management, TCP Sockets, UDP Sockets, Serial Bridging, Modem Emulation, and a Custom profile.
- The Digi Device Setup Wizard is intended to be run only once, and is not installed on a user's PC.

Disadvantages of the Digi Device Setup Wizard as an interface include:

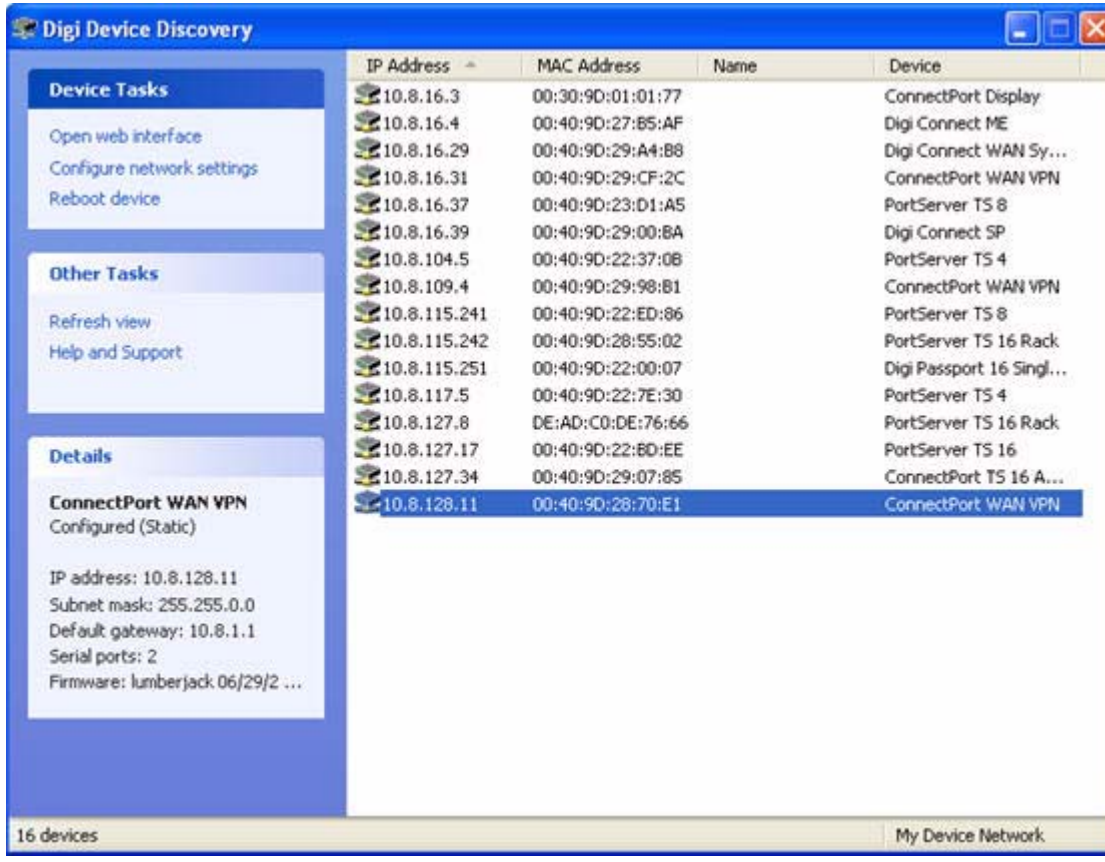
- While the wizard is available in Microsoft Windows or UNIX platforms, it requires Microsoft Windows for full support, and the PC running Windows usually needs to be on same network segment as the Digi Connect Family device. The Unix version of the Wizard does not include all the features of the Windows version. The Unix version is limited to network configuration settings, and does not allow configuring or choosing a scenario through port profiles.
- Some sites disallow users from running wizards, which would prevent users at such sites from using this interface.
- While the configuration capabilities of the Digi Device Setup Wizard are acceptable for most Digi Connect Family users, it only provides for the most common configuration scenarios, and is not as flexible as configuring through the Web user interface or the command line.
- The device discovery responses can be blocked by personal firewalls, VPN software, and certain network equipment. Disabling personal firewalls is not always possible.

To access the Digi Device Setup Wizard, insert the Software and Documentation CD that accompanies the Digi Connect Family device in a PC's CD drive. The Digi Device Setup Wizard will automatically start.

See "Configuration through the Digi Device Setup Wizard" on page 68 for details on running the wizard. The Digi Device Setup Wizard has online help, accessed from the Help button on wizard screens.

Digi Device Discovery Utility

The Digi Device Discovery Utility can be used to locate a Digi Connect Family device and open its Web user interface. It uses the Advanced Digi Discovery Protocol (ADDP), a Digi International-proprietary protocol for discovering devices on networks, to discover the Digi devices on a network, and displays the discovered devices in a list, as shown below.



Advantages of the Digi Device Discovery Utility are:

- It quickly locates Digi devices and basic device information, such as the device's address, firmware revision, and whether it has been configured.
- ADDP runs on any operating system capable of sending multicast IP packets to a network. ADDP sends out a User Datagram Protocol (UDP) multicast packet to all devices on the network. Devices that support ADDP reply to this UDP multicast with their configuration information. This means that even devices that do not yet have an IP address assigned, or that are misconfigured for the subnet, can reply to the UDP multicast packet, and be displayed in the device discovery results.

Disadvantages include:

- Device discovery responses can be blocked by personal firewalls, Virtual Private Network (VPN) software, and certain network equipment in place. Firewalls will block UDP ports 2362 and 2363 that ADDP uses to discover devices.
- Not all Digi devices support ADDP.

The Digi Device Discovery Utility is available on the Software and Documentation CD that accompanies the Digi device. After installing the utility, it is available from the **Start** menu.

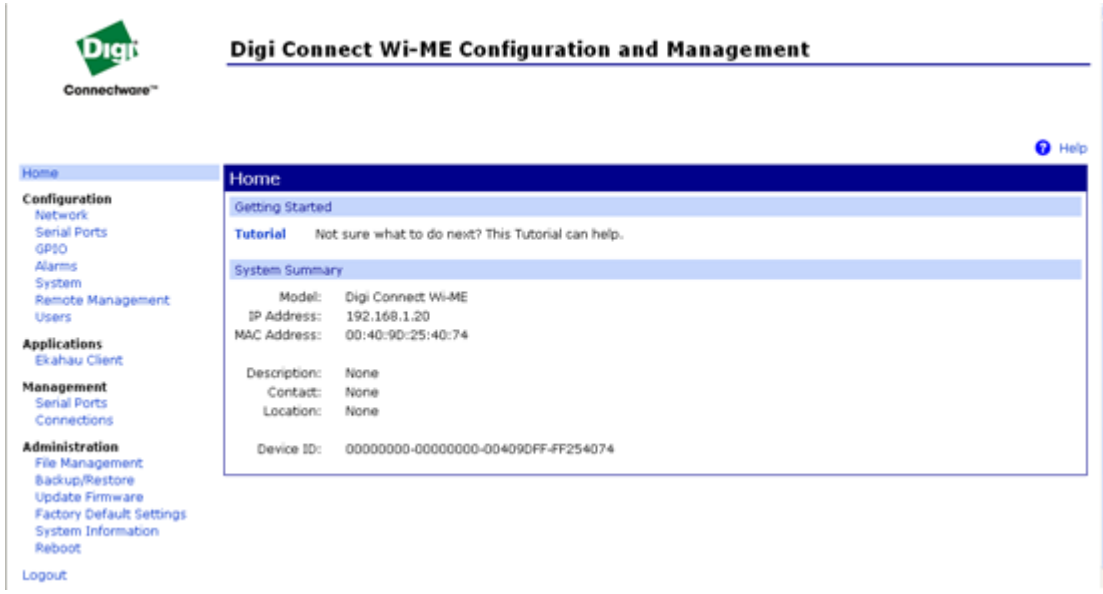
Access to the ADDP service can be enabled or disabled, but the network port number for ADDP cannot be changed from its default.

For more information on the Digi Device Discovery Utility, see page 72.

The Web User Interface

A Web user interface is provided as an easy way to configure and monitor Digi Connect Family products. Configurable features are grouped into several categories. These categories vary by product; examples include Network, Serial Port, GPIO (for all products except Digi Connect SP, Digi Connect Wi-SP), Alarms, System, Remote Management, UsersSecurity. Most of the configurable features are arranged by most basic settings on a page, with associated and advanced settings accessible from that page. As in the Digi Device Setup Wizard, serial-port configurations are classified into port profiles, or configuration scenarios that best represents the environment in which the Digi device will be used. Selecting a particular port profile configures the serial port parameters that are needed.

For some features, it may be desirable to establish a basic configuration using the Digi Device Setup Wizard, and then fine-tune the configuration using the Web user interface.



Advantages of the Web user interface include

- Ease of use, including point-and-click functionality and wizards that make configuration quick and complete.
- Secure access to devices.
- No need for programming experience.
- Port profiles simplify the configuration process.

A potential disadvantage of the Web user interface is that not all settings provided by the command-line interface are displayed. However, the configuration settings in the Web user interface should be sufficient for most users. If necessary, settings can be modified later from the command line.

To access the Web user interface, enter the Digi Connect Family device's IP address or host name in a browser's URL window. The main menu of the web interface is displayed.

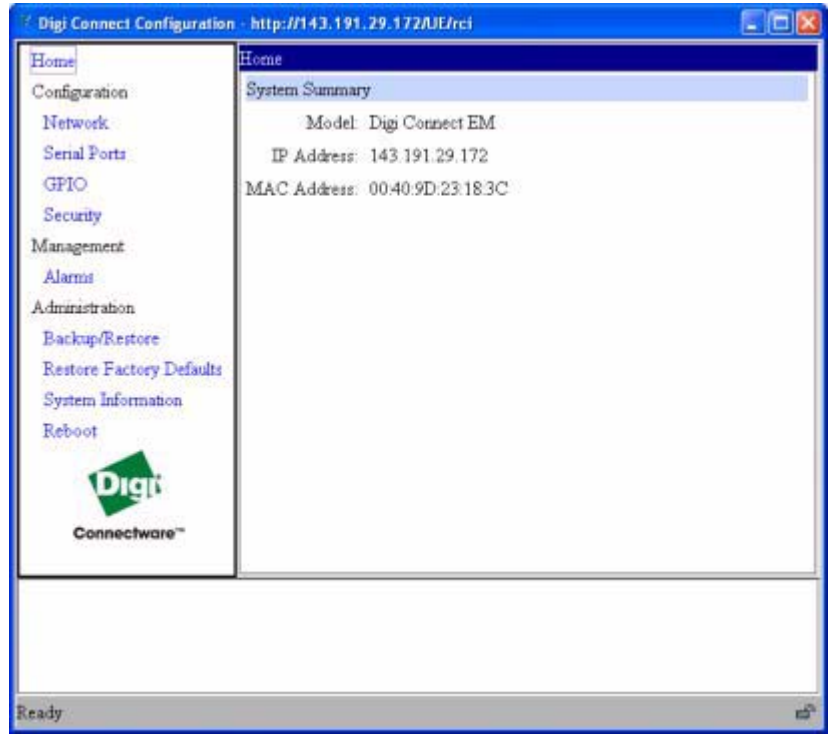
For more information, see "Configuration through the Web User Interface" on page 71.

The Web user interface has a tutorial, accessed from the Home page, and online help, accessed from the Help link on each page.

Java Applet Interface

An alternative configuration interface is provided with Digi Connect Family products, in the form of a Java applet. This interface provides many, but not all, of the configuration choices available through the Web user interface.

The Java applet is primarily intended as a sample alternative interface for embedded products. Embedded product manufacturers can use the applet as a base for their custom user interface. Because the interface is customizable, embedded product manufacturers can use it to provide a totally unique user interface that represents the kind of device in which the Digi Connect Family device is being embedded. For example, the configuration interface for a printer would look nothing like the Web user interface. Today, the only way to create a totally custom interface to the device is through an applet or other Remote Command Interface (RCI) application. The applet can be slightly modified using a configuration file, or it can be changed extensively. In addition, it can be used as a sample by those customers who choose to writer their custom configuration user interface from scratch.



Using the Java applet interface to configure devices provides the following advantages:

- A completely customizable interface. For example, the web interface can be changed by replacing the Digi logo with your company logo or changing the colors used in the interface workspace.
- The Java applet can also be used as a basis for further interface development. That is, if the Java applet is adequate for most configuration needs, but needs some modifications, the applet's operation can be customized. If a totally unique user interface is desired, the Java applet can serve as a sample program and a starting point from which to build new interfaces. It illustrates such concepts as configuring various aspects of the device using the RCI, applet packaging, and Swing user interface. Custom management applications can be written in other languages that run on a separate system in the network and talk to the device using RCI. For example, a printer manufacturer might have a configuration utility written in C++ that is installed on the PC along with the print driver.

Disadvantages of the Java applet interface include:

- The Java applet requires that the Sun Java Runtime environment be loaded.
- The Java applet does not allow for configuration of as many features as the Web user interface.
- The Java applet interface is essentially frozen, and will not be updated with additional configurable features or values in future releases.
- There is limited online help for the Java applet configuration screens. For more information on configurable areas, fields, and selectable values, review the online help for the Web user interface.

Access the Java applet interface from the User Interface section of the Home page of the Web user interface. Either click the **Launch** button next to the **Custom Interface** option, or click the **Set as Default** to set the Java applet as the default device interface. In some cases, a Digi device's default device interface may have already been preset to the Java applet by a system administrator.

See Chapter 2, "Configure Digi Connect Family Devices" for more information on using the Java applet to configure devices. While that chapter primarily focuses on configuring Digi Connect Family devices from the Web user interface, it also covers configuration from the Java applet, primarily the differences from the Web user interface.

Command-Line Interface

Digi Connect Family products can be configured by issuing commands from the command line. The command-line interface allows communication directly without a graphical interface. For example, the following is a command issued from the command line to set general serial configuration options:

```
#> set serial baudrate=9600 flowcontrol=hardware
```

Advantages of the command-line interface include:

- Flexibility. Although the command-line Interface is for experienced users and considered complex, it allows flexibility for precise configuration alterations.
- Direct communication to device or system.

Disadvantages of the command-line interface include:

- Users must have experience issuing commands.
- Command documentation is required.
- The command line allows the greatest flexibility to configure Digi devices, but is also considered complex.

The command line is available through Telnet or SSH TCP/IP connections, or through serial port using terminal emulation software such as Hyperterminal. Access to the command line from serial ports depends on the port profile in use by the port. By default, serial port command-line access is allowed.

See "Configuration through the Command Line" on page 134 for more information on this interface. See the *Digi Connect Family Command Reference* for command descriptions and examples of entering configuration commands from the command-line interface. In addition, online help is available for the commands, through the help and '?' commands.

Connectware Manager Interface

Connectware Manager is an optional, centralized device and network management package. From the Connectware Manager interface, you can:

- Configure devices
- Remotely upgrade device firmware
- Remotely reboot devices
- Reset devices to factory defaults
- Backup/restore device configuration properties
- Import or export the device configuration properties.
- Track devices
- Monitor devices and connections
- Set filters and send alarms
- Collect and analyze traffic information
- Manage the Connectware Manager server, including shutting down, stopping, restarting, and reconfiguring the server, and displaying reports and logs on server activity.

Advantages of the Connectware Manager interface are:

- Allows multiple devices to be managed (configured and monitored) from one source.
- The server can also be managed from same location.
- Logs and reports can be generated and reviewed. Summaries or totals can be linked back to the original devices for more thorough investigations.

Disadvantages include:

- Devices must be provisioned (assigned an IP address) before they can be accessed on Connectware Manager. Use the Digi Device Setup Wizard to provision devices.
- If used to manage a device, some of the device configuration options that are available on other device configuration interfaces, such as the Web and command-line interfaces, will not be available.
- To minimize network traffic, Connectware Manager uses caching. As a result, device settings can be out-of-sync between the device and the settings viewed on the Connectware Manager console.
- Connectware Manager requires a dedicated computer to act as a Connectware Manager server.

For more information on Connectware Manager as an remote management interface, see these resources:

- "Configure Remote Management (Connectware Manager Settings)" on page 109. This section shows how to configure Connectware Management settings within Digi devices.
- "Monitoring Capabilities from Connectware Manager" on page 153
- *Connectware Manager Getting Started Guide*
- *Connectware Manager Operator's Guide*
- Online help for Connectware Manager

Remote Command Interface (RCI)

Remote Command Interface (RCI) is a programmatic interface for configuring and controlling Digi Connect Family products. RCI is an XML-based request/response protocol that allows a caller to query and modify device configurations, access statistics, reboot the device, and reset the device to factory defaults. Unlike other configuration interfaces that are designed for a user, such as the command-line or Web user interfaces, RCI is designed to be used by a program. RCI access consists of program calls. A typical use of RCI is in a Java applet that can be stored on the Digi Connect Family device to replace the Web user interface with a custom browser interface. Another example is a custom application running on a PC that monitors and controls an installation of many Digi Connect Family devices.

As RCI is designed to be used by a program, it is useful for creating a custom configuration user interface, or utilities that configure or initialize devices through external programs or scripts.

Using RCI as a device configuration interface presents these disadvantages:

- RCI uses HTTP as the underlying transport protocol. Depending on the network configuration, use of HTTP as a transport protocol could be blocked by some firewalls.
- RCI is quite complex to use, requiring users to phrase configuration requests in Extensible Markup Language (XML) format. It is a “power-user” option, intended more for users developing their own user interfaces, or for users implementing embedded control (and thus potentially using RCI over serial) than for end-users with limited knowledge of device programming.
- Not all actions in the Web user interface have direct equivalents in RCI. Therefore, it may not be easy for some end-users to determine what needs to be sent through XML for a particular style of request.

For more details on RCI, see the Digi Connect Integration Kit and the *Remote Command Interface (RCI) Specification.*

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a protocol for managing and monitoring network devices. The SNMP architecture enables a network administrator to manage nodes--servers, workstations, routers, switches, hubs, etc.--on an IP network; manage network performance, find and solve network problems, and plan for network growth. Digi Connect Family products support SNMP Version 1.

Advantages of SNMP include:

- SNMP is easy to implement in extensive networks.
- Programming new variables is easy.
- SNMP is widely used. SNMP is a standard interface that integrates well with network management stations in an enterprise environment. While its capabilities are limited to device monitoring and display of statistics in Digi Connect Familydevices, read/write capabilities are expected to be added to Digi Connect Family devices in future releases.
- It is easy to 'drop in' new devices.

Disadvantages include:

- As device communication is UDP-based, the communication is not secure. If more secure communications with a device are required, an alternate interface must be used.
- SNMP does not allow for certain task that can be performed from the Web user interface, such as file management, uploading firmware, or backing up and restoring configurations.
- Compared to the Web or command-line interfaces, SNMP is limited in its ability to set specific parameters, such as set port profile, is not possible.

Accessing the SNMP interface requires a tool, such as a network management station. The management station relies on an agent at a device to retrieve or update the information at the device, including Device configuration, status, and statistical information. This information is viewed as a logical database, called a Management Information Base (MIB). MIB modules describe MIB variables for a variety of device types and computer hardware and software components.

Standard MIBs supported

The standard MIBs supported in Digi Connect Family devices are:

- MIB-II (RFC 1213) This is a MIB for managing a TCP/IP network. It is an update of the original MIB, now called MIB-I. MIB-II contains variable definitions that describe the most basic information needed to manage a TCP/IP network. These variable definitions are organized into several groups, such as groups for managing the system, network interfaces, address translation, transmission media, and various protocols, including IP, ICMP, TCP, UDP, EGP, and SNMP.
- CHARACTER-MIB (RFC 1658)
- RS-232-MIB (RFC 1659).

Digi enterprise MIBs supported

In addition to the standard MIBs, Digi Connect Family devices use several Digi enterprise MIBs, including:

- DIGI-DEVICE-INFO.mib: for handling device information. This MIB gives access to elements like the firmware revision, device name, IP network information, memory, and CPU statistics.
- DIGI-SERIAL-ALARM-TRAPS.mib: for handling alarms sent as SNMP traps.

Additional SNMP resources

A variety of resources about SNMP are available, including reference books, overviews, and other files on the Internet. For an overview of the SNMP interface and the components of MIB-II, go to **www.rfceditor.org**, and search for **MIB-II**. From the results, locate the text file describing the SNMP interface, titled *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*. The text of the Digi enterprise MIBs can also be displayed.

For additional discussion of using SNMP as a device monitoring interface, see "Monitoring Capabilities from SNMP" on page 154.

Monitoring Capabilities and Interfaces

There are several capabilities and interfaces for monitoring Digi Connect Family products; these are covered in more detail in Chapter 3, "Monitoring Capabilities".

Monitoring Capabilities

Monitoring Digi Connect Family products includes such tasks as checking device status, viewing information on a device's GPIO pins, checking runtime state, viewing serial port operations, and reviewing network statistics.

Monitoring Interfaces

As with device configuration, there are several interfaces available for monitoring Digi Connect Familyproducts, including:

- The Web user interface embedded with the product
- The optional Java applet
- SNMP
- The command-line interface
- Connectware Manager

Web and Java Applet User Interfaces

The Web user interfaceand the optional Java applet interface have several screens for monitoring Digi Connect Familydevices:

- Network Status
- Serial Port Management: for each port, the port's description, current profile, and current serial configuration.
- Connections Management: A display of all active system connections.

- System Information:
  - General device information
  - Current GPIO pin states
  - Serial port information: for each port, the port's description, current profile, and current serial configuration. This is the same information displayed by choosing Serial Port Management.
  - Network statistics: statistics for IP, TCP, UDP, and ICMP

Command-Line Interface

Several commands can be issued from the command line to monitor devices. For a review of these commands and what they can provide from a device-monitoring perspective, see "Monitoring Capabilities from the Command Line" on page 150.

Connectware Manager

In the Connectware Manager interface, monitoring capabilities can be sorted by the server and the devices managed by the server. The information is available in logs and can be generated into reports. When available, the reports post linked totals that can be drilled back to the original devices that make up the activity of the report.

SNMP

Monitoring capabilities of SNMP include managing network performance, gathering device statistics, and finding and solving network problems. For more information on using SNMP for device-monitoring purposes, see "Monitoring Capabilities from SNMP" on page 154.

Administration Tasks

Periodically, administrative tasks need to be performed on Digi Connect Family devices, such as:

- Uploading and managing files
- Changing the password for logging onto the device
- Backing up and restoring the configuration
- Updating firmware
- Restoring the configuration to factory defaults
- Rebooting the module

As with configuration and monitoring tasks, administration can be done from a number of interfaces, including the Web user interface, command line, and Connectware Manager. See Chapter 4, "Administration Tasks" for more information and procedures.

Configure Digi Connect Family Devices

C H A P T E R 2

This chapter describes how to configure a Digi Connect Family device. It covers these topics:

- "Alternate Methods for Assigning an IP Address" on page 64, which describes alternate methods for assigning an IP address to a Digi Connect Family device.
- "Configuration through the Digi Device Setup Wizard" on page 68.
- "Configuration through the Web User Interface" on page 71.
- "Alternative Configuration Options for Digi Connect Wi-SP" on page 124
- "Configuration through the Java Applet Interface" on page 128
- "Configuration through the Command Line" on page 134.
- "Configuration through Simple Network Management Protocol (SNMP)" on page 137.
- "Batch Capabilities for Configuring Multiple Devices" on page 137.

The primary focus of this chapter is on configuring Digi devices through the Web user interface. To use the Digi Device Setup Wizard for initial configuration, see the online help for the Wizard. For instructions on launching the wizard, see "Configure the IP Address Using the Digi Device Setup Wizard" on page 64.

Alternate Methods for Assigning an IP Address

There are several ways to assign an IP address to a Digi Connect Family device:

- Using the Digi Device Setup Wizard.
- Using Dynamic Host Configuration Protocol (DHCP) from the Web user interface.
- Using the command-line interface.
- Using Automatic Private IP Addressing (APIPA), also known as Auto-IP.

Configure the IP Address Using the Digi Device Setup Wizard

The Digi Device Setup Wizard is supplied on the Software and Documentation CD. Using this wizard is the easiest way to assign an IP address and initially configure Digi Connect Family products. It discovers Digi devices on a network, configures an IP address, and configures basic serial port parameters according to how the device will be used. After this initial configuration, features can be fine-tuned as needed through the Web user interface. Setup is specially designed for the Windows environments, and is quick, automated, and complete.

To use the Digi Device Setup Wizard:

1. Connect the Digi Connect Family device is connected to the network and power it on.
2. Locate the MAC address for the Digi Connect Family product. The MAC address is located on the label on the bottom of the product. Record it for later use in assigning an IP address.
3. Insert the Digi CD in the CD drive of a computer running Microsoft Window. If the CD does not start automatically, double-click **My Computer > CD ROM Drive > setup.exe**.
4. The Digi Device Setup Wizard automatically starts. Select the appropriate platform and click **Next**.

   The Digi device discovery utility finds and lists all of the Digi devices on the network.
5. Locate the Digi Connect Family device by its MAC address.

6 Select the Digi Connect Family device and then click **Next**.

7 Follow the instructions in the wizard to assign an IP address for the Digi Connect Family device. Use the online help supplied with the wizard for information about values and selections on the wizard screens. For additional information about configuration settings displayed on the wizard screens, continue to "Configuration through the Digi Device Setup Wizard" on page 68.

Configure the IP Address Using DHCP

A IP address can also be configured using Dynamic Host Configuration Protocol (DHCP).

Procedure

This procedure assumes that the Digi Connect Family device is configured as a DHCP client. Since this is the default configuration, this will be the case unless the configuration has been changed.

1 Make sure the Digi Connect Family device is not powered on.

2 If desired, set up a permanent entry for the Digi Connect Family device on a DHCP server. While this is not necessary to obtain an IP address via DHCP, setting up a permanent entry means the IP address will be saved after the device is rebooted.

3 Connect the Digi Connect Family device to the network and power it on. The IP address configured in step 2 is assigned automatically.

Configure the IP Address using Auto-IP

The standard protocol Automatic Private IP Addressing (APIPA or Auto-IP) assigns the IP address from the reserved IP addresses in Auto-IP. Use ADDP or DHCP to find the device and assign it a new IP address that compatible with your network. Once the unit is plugged in, Auto-IP automatically assigns the IP address.

Configure the IP Address from the Command-Line Interface

The **set network** command configures an IP address from the command line. Include the following parameters:

- **ip=*device ip***: The IP address for the device.
- **gateway=*gateway***: The network gateway IP address.
- **submask=*device submask***: The device subnet mask.
- **dhcp=off**: Turns off use of the Dynamic Host Configuration Protocol (DHCP), so that the IP address assigned is permanent.
- **static=on**: Specifies that the IP address is static, and will remain as the specified IP address, gateway, and submask.

For example:

```
set network ip=10.0.0.100 gateway=10.0.0.1
submask=255.255.255.0 dhcp=off static=on
```

To configure the Digi Connect SP through the command line, the DIP switches must be changed. See "Command Line Access" on page 124 for an illustration of the DIP switch settings.

IP Addresses and Connectware Manager

The Connectware Manager interface can only change the Ethernet/LAN address for a Digi Connect Family device. To change the IP address, open the Web user interface for based on the IP address the device has and navigate to **Configuration > Network > IP Settings**. On the IP Settings page, enter the new IP address, subnet mask, and gateway.

To use Connectware Manager, first configure the Digi device using the Digi Device Setup Wizard, then install Connectware Manager. For more information, see the *Connectware Manager Operator's Guide*.

Test the IP Address Configuration

Once the IP address is assigned, test the IP address configuration to be sure it works as configured. This procedure assumes that the Digi Connect Family device an IP address.

1 Access the command line of a PC or other networked device.

2 Issue the following command:

```
ping ip-address
```

where *ip-address* is the address assigned to the Digi Connect Family device. For example:

```
ping 192.168.2.2
```

Configuration through the Digi Device Setup Wizard

The Digi Device Setup Wizard helps configures Digi devices according to one of several port profiles, or configuration scenarios that characterize the manner in which your Digi product will be used. Depending on the Digi device, the wizard configures several other features.

To run the Digi Device Setup Wizard, insert the Software & Documentation CD packaged with your Digi Connect Family product. The first screen of the wizard is displayed. Click **Next.**

Discover the Device

The **Discover Device** screen displays a list of Digi devices that have been discovered on the network. Locate the Digi Connect Family device to configure, and double-click it.

Device discovery responses can be blocked by personal firewalls, VPN software, and certain network equipment in place. Firewalls will block UDP ports 2362 and 2363 that the Advanced Digi Discovery Protocol (ADDP) uses to discover devices.

Configure Network Settings

The **Configure Network Settings** screen sets how the IP address settings are established for the Digi Connect Family device.Either choose to obtain the network settings automatically using DHCP, or manually enter them.

Install RealPort Software

RealPort software must be installed and configured on each PC that uses the RealPort ports on the Digi Connect Family device. This RealPort software is available on the Software and Documentation CD and can be loaded from the Digi Device Setup Wizard. To install RealPort, make sure the **Install Digi RealPort on this computer** checkbox is selected.

Use Port Profiles to Configure Serial Port Settings

The Digi Device Setup Wizard configures a serial port based on the way the port will be used. This is done by associating a port profile with the port. Port profiles are a defined set of serial port parameters for a particular use. There are several port profile choices; the complete list is below, but support can vary among Digi products. If a profile is not displayed on the selection screen in the wizard, the Digi device not support that use of the serial port.

- **RealPort**: Maps a COM or TTY port to the serial port.
- **Console Management**: Accesses a device's console port over a network connection.
- **TCP Sockets**: Allows a serial device to communicate over a TCP network.
- **UDP Sockets**: Allows a serial device to communicate using UDP.
- **Serial Bridge**: Configures one side of a serial bridge. A bridge connects two serial devices over the network, as if they were connected with a serial cable.
- **Local Configuration:** For connecting a terminal to the serial port to access the device console port.
- **Modem Emulation**: Configures the serial port to act as a modem.
- **Custom**: An advanced option to allow full configuration of the serial port. This profile displays all settings associated with the serial port.

Verify Configuration Settings

On the **Verify Configuration** screen, clicking **Next** shows the configuration settings that will be uploaded to the Digi Connect Family device.

Save Settings

The **Save Settings** page is displayed while the configuration settings are uploaded to the Digi Connect Family device.Other messages and wizards may be displayed during this step; click **OK** on message boxes and **Next** on wizard screens to continue the installation process.

Finish the Wizard and Select Next Action

When the configuration settings have been uploaded to the Digi Connect Family device, a **Finish** screen is displayed. There are several options for what to do next, including registering the device, opening other device interfaces such as the Web user interface or command line interface to further configure it, or configuring another Digi device. Click **Finish** to close the wizard.

To Further Configure the Digi Connect Device

Once a Digi Connect Family device is configured through the Digi Device Setup Wizard, or if the Digi Device Setup Wizard fails to complete for any reason, as needed, use one of the other device interfaces to view and change the configuration. For example, open the Web user interface or the optional Java applet interface, and change configuration settings there, or access the command-line interface and enter commands to display and change configuration settings. For more information on using these interfaces, see "Configuration through the Web User Interface" on page 71, "Configuration through the Java Applet Interface" on page 128, and "Configuration through the Command Line" on page 134.

Configuration through the Web User Interface

Configuring Digi Connect Family devices through the Web user interface involves these tasks:

- Change the IP address, as needed. See page 77.
- Open the Web interface. See page 72.
- Configure network communications. See page 78.
- Configure the serial ports. See page 91.
- Configure GPIO pins. Not supported in Digi Connect SP, Digi Connect Wi-SP. See page 100.
- Configure alarms. See page 104.
- Configure security/user features such as user names and password authentication. See page 114.
- Configure system-identifying information and the settings for Simple Network Management Protocol (SNMP). See page 108.
- Configure remote management using a Connectware Manager server. See page 109.
- Configure and run applications available for use. Supported applications vary. See page 121.

Open the Web Interface

To open the Web user interface, either enter the Digi Connect Family device's URL in a Web browser and log on to the device, if required, or use the Digi Device Discovery utility to locate it and open its Web interface.

By Entering the Device's URL in a Web Browser

1. In the URL address bar of a Web browser, enter the IP address of the device.
2. If security has not been enabled for the Digi Connect Family device, the Home page of the Web user interface is displayed. If security has been enabled for the device, a login dialog will be displayed. Enter the user name and password for the device. The default username is **root** and the default password is **dbps**. If these defaults do not work, contact the system administrator who set up the device. Then the Home page of the Web user interface is displayed. See "Organization of the Web Interface" on page 74 for an overview of using the Home page and other linked pages.

   Note The idle timeout automatically logs users out of the web user interface after 5 minutes of inactivity if password authentication has been enabled for the device.

By Using the Digi Device Discovery Utility

Alternatively, use the Digi Device Discovery Utility to locate the Digi Connect Family device and open the Web user interface.

Install the Digi Device Discovery Utility

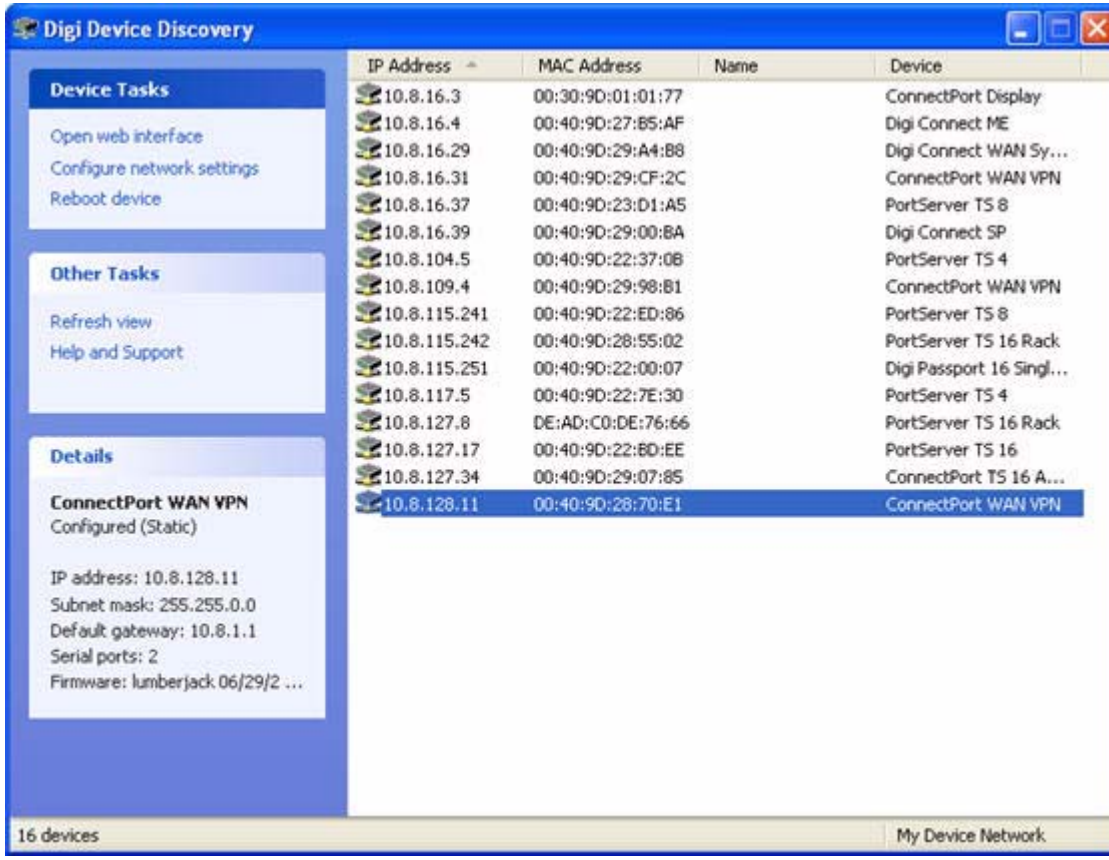
The Digi Device Discovery Utility is available on the Software and Documentation CD. If this utility is not already available on your computer, follow these steps.

1. On the main page Software and Documentation CD, click **software - install optional software**.
2. Select **Device Discovery Utility** and click **Install**.
3. Follow the prompts of the Setup Wizard to install the Digi Device Discovery Utility software.

Discover Devices

From the start menu, select **Start > Programs > Digi Connect > Digi Device Discovery**. The Digi Device Discovery application is displayed.

Locate the device in the list of devices, and double-click it, or select the device from the list and select Open web interface in the Device Tasks list.

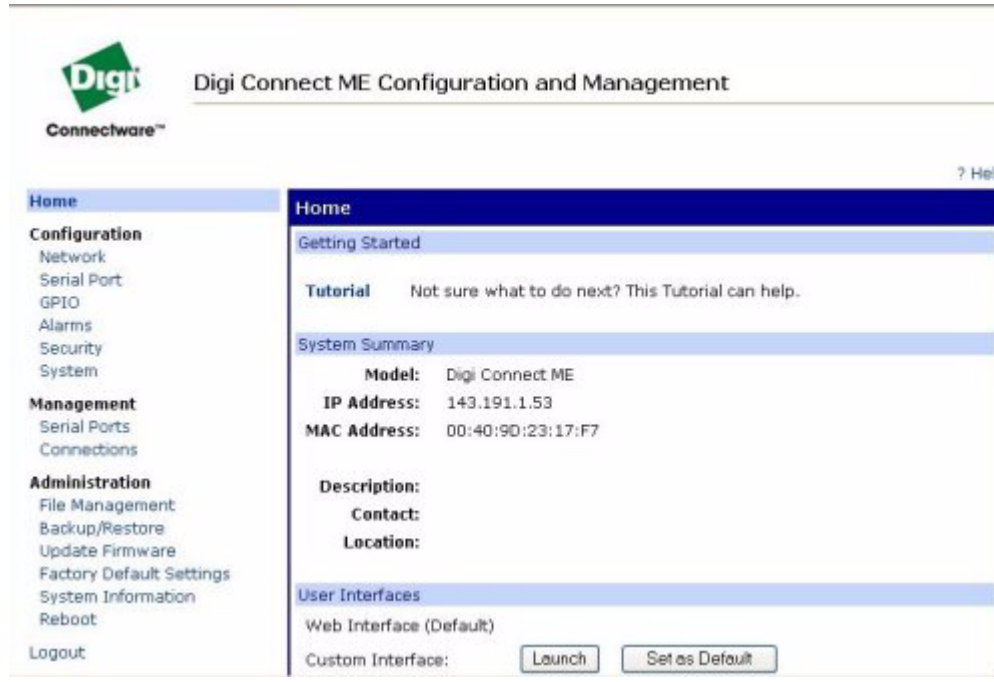


4 Depending on whether a system administrator has configured password authentication for the device, a login may be required. If a login dialog is displayed, enter the user name and password for the device. The default username is **root** and the default password is **dbps**. If these defaults do not work, contact the system administrator who initially set up the device. Now configure the device, as described on the following pages.

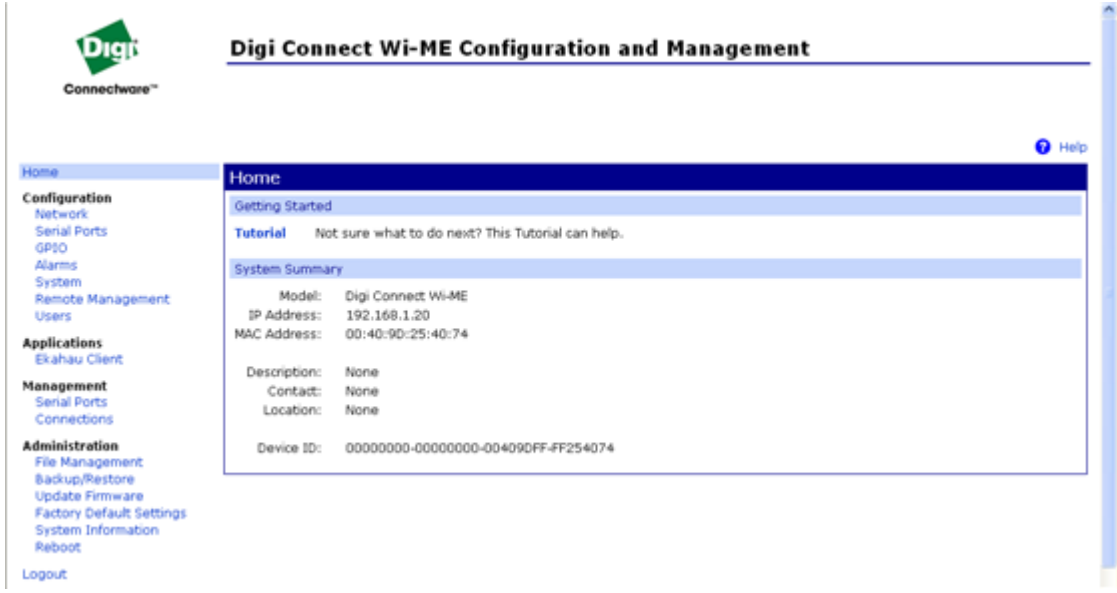
Organization of the Web Interface

When Web user interface is opened, the Home page is displayed.

Here is the home page for Digi Connect ME:



And here is the Home page for a Digi Connect Wi-ME. Note the additional **Application** menu item.



The Home Page

The left side of the Home page has a menu of choices that display pages for configuration, management, and administration tasks, and to log out of the Web user interface. This chapter focuses on the choices under **Configuration** and **Application**. For details on monitoring Digi devices and the choices under **Management**, see Chapter 3, "Monitoring Capabilities". For details on the tasks under **Administration**, see Chapter 4, "Administration Tasks".

Clicking **Logout** logs out of a configuration and management session with a Digi Connect Family device. It does not close the browser window, but displays a logout window. To finish logging out of the Web user interface and prevent access by other users, close the browser window. Or, log back on to the device by clicking the link on the screen. After 5 minutes of inactivity, the idle timeout also automatically performs a user logout.

The **Getting Started** section has a link to a tutorial on configuring and managing Digi Connect Family devices.

The **System Summary** section notes all available device-description information.

Configuration Pages

The choices under **Configuration** in the menu display pages for configuring settings for various features, such as network settings, and serial port settings.

Some of the configuration settings are organized on sets of linked screens. For example, the Network Configuration screen initially displays the IP Settings, and provides links to Network Services Settings, Advanced Settings, and other network settings appropriate to the Digi device.

Application Pages

Depending on the Digi product, there may be an **Application** menu item for configuring various applications available for use with your Digi Connect product.

- **Ekahau Client:** For Digi Connect wireless device, configures Ekahau Client™ device-location software. See page 121.

Apply and Save Changes

The Web user interface runs locally on the device, which means that the interface always maintains and displays the latest settings in the Digi Connect Family device.

On each screen, the **Apply** button is used to save any changes to the configuration settings to the Digi Connect Family device.

Cancel Changes

To cancel changes to configuration settings, click the **Refresh** or **Reload** button on the Web browser. This causes the browser to reload the page. Any changes made since the last time the **Apply** button was clicked are reset to their original values.

Restore the Device to Factory Defaults

The device configuration can be reset to factory defaults as needed during the configuration process. See "Restore a Device Configuration to Factory Defaults" on page 160.

Online Help

Online help is available for all screens of the Web user interface, and for common configuration and administration tasks. There is also tutorial available on the Home page.

Change the IP Address from the Web User Interface, As Needed

Normally, IP addresses are assigned to Digi products either through DHCP or the Digi Device Setup Wizard.

This procedure assumes that the Digi device already has an IP address and you simply want to change it.

1. Open a web browser and enter the Digi Connect Family device's current IP address in the URL address bar.
2. If security is enabled for the Digi Connect Family device, a login prompt is displayed. Enter the user name and password for the device. The default username is **root** and the default password is **dbps**. If these defaults do not work, contact the system administrator who set up the device.
3. Click **Network** to access the Network Configuration page.
4. On the IP Settings page, select **Use the following IP address**.
5. Enter an IP address (and other network settings), then click **Apply** to save the configuration.

Configure Network Communications

The Network configuration pages include the following:

- **IP Settings:** For viewing IP address settings and changing as needed. See page 79.
- **Wireless LAN Settings:** For setting basic options such as network name and network connection options. See page 79.
- **Wireless Security Settings:** For setting authentication and encryption options. See page 79.
- **Wireless 802.1x Authentication Settings:** Detailed authentication settings for IEEE 802.1x authentication. See page 79.
- **Network Services Settings:** Enable and disables access to various network services, such as ADDP, RealPort and Encrypted RealPort, Telnet, HTTP/HTTPS, and other services. See page 84.
- **Advanced Network Settings**: Configures the Ethernet Interface speed and mode, TCP/IP settings, TCP keepalive settings, and DHCP settings. See page 90.

Alternatives for Configuring Network Communications

There are three ways a Digi Connect Family device can be configured on the network.

- **Using dynamic settings**: All network settings will be assigned automatically by the network, using a protocol called DHCP. Contact your network administrator to find out if a DHCP server is available.
- **Using static settings**: All network settings are set manually and will not change. The IP address and Subnet Mask are mandatory. The rest are not mandatory, but may be needed for some functions. Contact your network administrator for the required values.
- **Using Auto-IP**: Auto-IP assigns an IP address to the Digi device immediately after it is plugged in. If running DHCP or ADDP, the Auto-IP address is overridden and a network compatible IP address is assigned, or a static IP address can be assigned.

Even if a DHCP server is available, the device configuration may work better with static settings. Once set, static settings will not change, so you and other network devices can always find the Digi Connect Family device by its IP address. With dynamic settings, the DHCP server can change the IP address. This can happen frequently or infrequently depending on how your network administrator has configured the network.

When the IP address does change, you and other network devices configured to talk to the Digi Connect Family device can no longer access the device. In this case, the Digi Connect Family device must be located the Digi Device Discovery utility, and other network devices that need to communicate with the Digi Connect Family device must be reconfigured.

IP Settings

The IP Settings page shows how the IP address of the Digi Connect Family device is obtained, either by DHCP or by using a static IP address, subnet mask, default gateway. In addition, this page shows IP addresses of the primary and secondary Domain Name System (DNS) server for the Digi device. Contact your network administrator for more information about these settings, and see the online help.

Wireless LAN Settings

Digi Connect wireless devices contain a wireless network interface that may be used to communicate to wireless networks using 802.11b technology. Contact your administrator or consult your wireless access point documentation for the settings required to setup the wireless network configuration.

Wireless LAN settings include:

- **Network name:** The name of the wireless network to which the wireless device should connect. In situations with multiple wireless networks, this setting allows the device to connect to and associate with a specific network. The network name is referred to as the SSID (service set identifier). If the network name is left blank, the device will search for wireless networks and connect to the first available network. This is useful if a specific network name does not need to be used as the device will select the first available network.
- **Connection Options** The type of wireless connection the wireless network uses to communicate. These are the methods this device uses to communicate on wireless networks:
  - **Connect to any available wireless network:** Use this setting to allow the device to access any network. The device can either access point networks or peer-to-peer wireless networks.
  - **Connect to access point (infrastructure) networks only:** Use this setting if the wireless network that this device needs to connect to is composed of wireless access points. This is typically the most popular method for connecting to wireless networks.
  - **Connect to peer-to-peer (ad-hoc) networks only:** Use this setting if all devices on the wireless network connect to and communicate with each other. This is known as peer-to-peer in that there is no central server or access point. Each system communicates directly with each other system.
- **Country:** The country in which this wireless device is being used. The channel settings are restricted to the legal set for the selected country.
- **Channel:** The frequency channel that the wireless radio will use. Select Auto-Scan to have the device scan all frequencies until it finds one with an available access point or wireless network it can join.
- **Transmit Power:**
- **Enable Short Preamble:** Enables transmission of wireless frames using short preambles. If Short Preamble is supported in the wireless network, enabling it can boost overall throughput.
- **Enable Antenna Diversity:** Enables reception on multiple antennas. This is a means of improving overall signal reception.

Wireless Security Settings

Specify the wireless security settings that the wireless network uses. Multiple security and authentication modes may be chosen depending on the configuration of the access point or wireless network. The wireless device will automatically select and determine the authentication and encryption methods to use while associating to the wireless network. If the wireless network does not use security and uses an *Open Network* architecture, these settings do not need to be modified.

Note that WPA settings require that the device communicate to Access Points and is not valid when the **Connection Method** is set to **Connect to wireless systems using peer-to-peer (ad-hoc)**. Also, WPA pre-shared key (WPA-PSK) security is only valid when a specific **Network Name** or SSID is being used.

- **Network Authentication:** Multiple authentication methods can be selected. The **Any** option enables all of the methods. The actual method used will be determined by the capabilities of the wireless network.
  - **Open System:** IEEE 802.11 open system authentication is used to establish a connection.
  - **Shared Key:** IEEE 802.11 shared key authentication is used to establish a connection. At least one WEP key must be specified in order to use shared key authentication.
  - **WEP with 802.1x authentication:** IEEE 802.1x authentication (EAP) is used to establish a connection with an authentication server or access point. Wired Equivalent Privacy (WEP) keys are dynamically generated to encrypt data over the wireless network.
  - **WPA with pre-shared key (WPA-PSK):** The Wi-Fi Protected Access (WPA) protocol is used with a pre-shared key (PSK). The PSK is calculated using a passphrase and the network SSID.
  - **WPA with 802.1x authentication:** The WPA protocol and IEEE 802.1x authentication (EAP) is used to establish a connection with an authentication server or access point. Encryption keys are dynamically generated to encrypt data over the wireless link.
  - **Cisco LEAP:** Lightweight Extensible Authentication Protocol (LEAP) is used to establish a a connection with an authentication server or access point. Wired Equivalent Privacy (WEP) keys are dynamically generated to encrypt data over the wireless link. A user name and password must be specified to use LEAP.

- **Data Encryption:** Multiple encryption methods can be selected. The **Any** option enables all of the methods. The actual method used will be determined by the capabilities of the wireless network.
  - **Open System:** No encryption is used over the wireless link. Open System encryption is valid only with Open System and Shared Key authentication.
  - **WEP:** Wired Equivalent Privacy (WEP) encryption is used over the wireless link. WEP encryption can be used with any of the above authentication methods.
  - **TKIP:** Temporal Key Integrity Protocol (TKIP) encryption is used over the wireless link. TKIP encryption can be used with WPA-PSK and WPA with 802.1x authentication.
  - **CCMP:** CCMP (AES) encryption is used over the wireless link. CCMP can be used WPA-PSK and WPA with 802.1x authentication.
- **WEP Keys**
  - **Transmit Key:** Specify the corresponding key of the encryption key that should be used when communicating with wireless networks using WEP security.

    This device allows up to four wireless keys to be set of either 64-bit or 128-bit encryption. These keys allow the wireless network to traverse different wireless networks without having to change the wireless key. Instead, only the transmit key setting has to be changed to specify which wireless key to send.
  - **Encryption Keys:** Specify 1 to 4 encryption keys to be used when communicating with wireless networks using WEP security.

    The encryption keys should be a set of 10 (64-bit) or 26 (128-bit) hexadecimal characters. The encryption key should only contain the characters A-F, a-f, or 0-9. Optionally, separator characters, such as '-', '_', or '.' may be used to separate the set of characters.
  - **Passphrase:** Specify the passphrase that the wireless network uses with WPA pre-shared keys. The pre-shared key is calculated using the passphrase and the SSID. Therefore, a valid network name must have been previously specified.
- **WPA PSK** (Pre-Shared Key)
- **Username/Password Used for Network Authentication:** Specify the username and password combination used to authenticate on the network when using LEAP or 802.1x authentication with PEAP or TTLS.

Wireless 802.1x Authentication Settings

- **EAP Methods:** These are the types of Extensible Authentication Protocols (EAP) or outer protocols that are allowed to establish the initial connection with an authentication server or access point. These are used with WEP with 802.1x authentication and WPA with 802.1x authentication.
  - **PEAP:** Stands for "Protected Extensible Authentication Protocol." A username and password must be specified to use PEAP.
  - **TLS:** Stands for "Transport Layer Security." A client certificate and private key must be installed in order to use TLS.
  - **TTLS:** Stands for "Tunneled Transport Layer Security." A username and password must be specified to use TTLS.
- **PEAP/TTLS Tunneled Authentication Protocols:** These are the types of inner protocols that can be used within the encrypted connection established by PEAP or TTLS.

  The following are **Extensible Authentication Protocols (EAP)** that can be used with PEAP or TTLS.
  - **GTC:** Generic Token Card
  - **MD5:** Message Digest Algorithm.
  - **MSCHAPv2:** Microsoft Challenge response Protocol version 2.
  - **OTP:** One Time Password

  The following are **non-EAP protocols** that can be used with TTLS.
  - **CHAP:** Challenge Response Protocol
  - **MSCHAP:** Microsoft Challenge response Protocol
  - **TTLS MSCHAPv2:** TTLS Microsoft Challenge response Protocol version 2.
  - **PAP:** Password Authentication Protocol

- **Client Certificate Use:** To use TLS, a client certificate and private key must be installed on the Digi device.
  - **Client Certificate:** Click **Browse** to select a client certificate file. Then click the next **Browse** to select a private key file. If the private key file is encrypted, a password must be specified.
  - **Verify server certificates:** Enable to verify that certificates received from an authentication server or access point are signed by a trusted certificate authority (CA). Standard CAs are built in. Additional trusted certificates may be added.
  - **Trusted Certificates:** To add additional trusted certificates, click **Browse** to select a certificate file to upload to the Digi device, then click **Upload**.
  - **Installed Certificates:** Shows which client certificates have been added and are in use.

Network Services Settings

The Network Services page shows a set of common network services that are available for Digi devices, and the network port on which the service is running.

Common network services can be enabled and disabled, and the TCP port on which the network service listens can be configured. Disabling services may be done for security purposes. That is, certain services can be disabled so the device runs only those services specifically needed. To improve device security, non-secure services such as Telnet can be disabled.

It is usually best to use the default network port numbers for these services because they are well known by most applications.

Several services have a setting for whether TCP keep-alives will be sent for the network services. TCP keep-alives can be configured in more detail on the **Advanced Network Settings** page.

Caution Exercise caution in enabling and disabling network services, particularly disabling them. Changing certain settings can render a Digi Connect device inaccessible. For example, disabling Advanced Digi Discovery Protocol (ADDP) prevents the device from being discovered on a network, even if it is actually connected. Disabling HTTP and HTTPS disables access to the Web user interface. Disabling basic services such as Telnet, Rlogin, etc. can make the Command-Line interface inaccessible.

Supported Network Services and Default Network Port Numbers

In Digi Connect products that have multiple serial ports, the network port number defaults for various services are set based on the following formula:

base network port number + serial port number

For example, the Telnet Passthrough service is set to network port 2001 for serial port 1, 2002 for serial port 2, 2003 for serial port 3, etc.

If a network port is changed for a particular service, that is the only network port number that changes. That change does not carry over to the other network ports. For example, if the network port number for Telnet Passthrough is changed from 2001 to 3001, that does not mean that the other network ports will change to 3002, 3003, etc.

There are two types of network services available:

- Basic services, which are accessed by connecting to a particular well-known network port.
- Passthrough services, in which a particular serial port is set up for a particular type of service. To use the service, users must both use the correct protocol and specify the correct network port. For example, assuming default service ports and using a Linux host, here is how a user would access the SSH and Telnet passthrough services:

```
#> ssh -l fred digi16 -p 2501
#> telnet digi16 2101
```

The following table shows the network services, the services provided, and the default network port number for each service.

Service	Services Provided	Default Network Port Number
Device Discovery, also known as Advanced Digi Discovery Protocol (ADDP)	Discovery of Digi Connect products on a network. Disabling this service disables use of the Digi Device Discovery utility to locate the device, either on its own or as part of running the Digi Device Setup Wizard. The network port number for ADDP cannot be changed from its default.	2362
Encrypted (Secure) RealPort	Secure Ethernet connections between COM or TTY ports and device servers or terminal servers.	1027
Line Printer Daemon (LPD)	Allows network printing over a serial port.	515
Modem Emulation Pool (pmodem)	Allows the Digi Connect product to emulate a modem. Modem emulation sends and receives modem responses to the serial device over the Ethernet instead of Public Switched Telephone Network (PSTN). Telnet processing can be enabled or disabled on the incoming and outgoing modem-emulation connections. The pmodem service is for connecting to whatever serial port will answer.	5000
Modem Emulation Passthrough	Allows the Digi Connect product to emulate a modem. This service is for dialing in to a particular serial port that has been set up for modem emulation.	5001
RealPort	A virtual connection to serial devices, no matter where they reside on the network.	771
Remote login (Rlogin)	Allows users to log in to the Digi Connect device and access the command-line interface through Rlogin.	513
Remote shell (Rsh)	Allows users to log in to the Digi Connect device and access the command-line interface through Rsh.	514

Service	Services Provided	Default Network Port Number
Secure Shell (SSH)	Allows users secure access to log in to the Digi Connect device and access the command-line interface.	22
Secure Shell (SSH) Passthrough	Accessing a specific serial port set up for SSH.	2501
Secure Socket Service	Authentication and encryption for Digi Connect devices.	2601
Simple Network Management Protocol (SNMP)	Managing and monitoring the Digi Connect device. To run SNMP in a more secure manner, note that SNMP allows for “sets” to be disabled.This securing is done in SNMP itself, not through this command. If disabled, SNMP services such as traps and device information are not used.	161
Telnet Server	Allows users an interactive Telnet session to the Digi Connect product’s command-line interface. If disabled, users cannot Telnet to the device.	23
Telnet Passthrough	Allows a Telnet connection directly to the serial port, often referred to as reverse Telnet.	2001
Transmission Control Protocol (TCP) Echo	Used for testing the ability to send and receive over a TCP connection, similar to a ping.	7
Transmission Control Protocol (TCP) Passthrough	Allows a raw socket connection directly to the serial port, often referred to as reverse sockets.	2101
User Datagram Protocol (UDP) Echo	Used for testing the ability to send and receive over a UDP connection, similar to a ping.	7
User Datagram Protocol (UDP) Passthrough	Allows raw data to be passed between the serial port and UDP datagrams on the network.	2101

Service	Services Provided	Default Network Port Number
Web Server, also known as HyperText Transfer Protocol (HTTP)	Access to web pages for configuration that can be secured by requiring a user login. HTTP and HTTPS, below, are also referred to as Web Server or Secure Web Server. These services control the use of the Web interface. If HTTP and HTTPS are disabled, device users cannot use the Web user interface or Java applet to configure, monitor, and administer the device.	80
Secure Web Server, also known as HyperText Transfer Protocol over Secure Socket Layer (HTTPS)	Access to web pages for configuration that can be secured by requiring a user login, with encryption for greater security.	443

Socket Tunnel Settings

A Socket Tunnel can be used to connect two network devices: one on the Digi Cellular Family device's local network and the other on the remote network. This is especially useful for providing SSL data protection when the local devices do not support the SSL protocol.

One of the endpoint devices is configured to initiate the socket tunnel. The tunnel is initiated when that device opens a TCP socket to the Digi Cellular Family device on the configured port number. The Digi Cellular Family device then opens a separate connection to the specified destination host. Once the tunnel is established, the Digi Cellular Family device acts as a proxy for the data between the remote network socket and the local network socket, regardless of which end initiated the tunnel.

Socket Tunnel settings include:

- **Enable:** Enables or disables the configured socket tunnel.
- **Timeout:** The timeout (specified in seconds) controls how long the tunnel will remain connected when there is no tunnel traffic. If the timeout value is zero, then no timeout is in effect and the tunnel will stay up until some other event causes it to close.
- **Initiating Host:** The hostname or IP address of the network device which will initiate the tunnel. This field is optional.
- **Initiating Port:** Specify the port number that the Digi Cellular Family device will use to listen for the initial tunnel connection.
- **Initiating Protocol:** The protocol used between the device that initiates the tunnel and the Digi Cellular Family device. Currently, TCP and SSL are the two supported protocols.
- **Destination Host:** The hostname or IP address of the destination network device.
- **Destination Port:** Specify the port number that the Digi Cellular Family device will use to make a connection to the destination device.
- **Destination Protocol:** This is the protocol used between Digi Cellular Family device and the destination device. Currently, TCP and SSL are the two supported protocols. This protocol does not need to be the same for both connections.

Advanced Network Settings

The Advanced Network Settings are used to further define the network interface, including:

- **Host name**: The Host name to be placed in the DHCP Option 12 field. This is an optional setting which is only used when DHCP is enabled.
- **Enable Auto IP address assignment**: Whether Auto-IP address assignment is enabled or disabled.
- **Ethernet Interface speed and duplex mode** (Auto, Half-Duplex, or Full Duplex).
- **TCP keep-alive settings**: The DHCP server assigns these network settings, unless they are manually set here. To manually set and override these settings, select **Ignore TCP Keep-Alive settings from DHCP** and specify the values for **Idle Timeout**, **Probe Interval**, and whether an extra byte should be stored in TCP keep-alive packets.
- **Maximum transmission rate**: For wireless products only, there is an advanced network setting of maximum transmission rate.

Configure Serial Ports

Use the Serial Port Configuration page to establish a port profile for the serial port of the Digi Connect Family device. The Serial Port Configuration page includes the currently selected port profile for the serial port, detailed configuration settings for the serial port, dependent on the port profile selected, and links to Basic Serial Settings and Advanced Serial Settings.

About Port Profiles

Port profiles simplify serial port configuration by displaying only those items that are relevant to the currently selected profile. If the Digi Device Setup Wizard was used to initially configure the Digi device, the wizard prompted to select a port profile.

There are several port profile choices for the Digi Connect Family Support of port profiles varies by Digi product. If a profile listed here is not available on the page, it is not supported in the Digi product.

If a port profile has already been selected, it is shown at the top of the screen. The profile can be changed, or retained but individual settings adjusted.

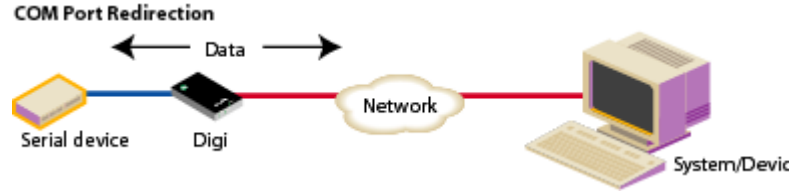
Everything displayed on the Serial Port Configuration screen between **Port Profile Settings** and the links to the **Basic Serial Settings** and **Advanced Serial Settings** depends on the port profile selected.

Select and Configure a Port Profile

1. To configure any profile select **Serial Ports.**
2. Click the port to be configured.
3. Click **Change Profile.**
4. Select the appropriate profile and Click **Apply**.
5. Enter the appropriate parameters for each profile. Descriptions of each profile follow. See also the online help for the configuration screens for more details about settings and values.
6. Click **Apply** to save the settings.

RealPort Profile

The RealPort Profile maps a COM or TTY port to a serial port. This profile configures a Digi device to create a virtual COM port on a PC, known as COM Port Redirection. The PC applications send data to this virtual COM port and RealPort sends the data across the network to the Digi Connect Family device.

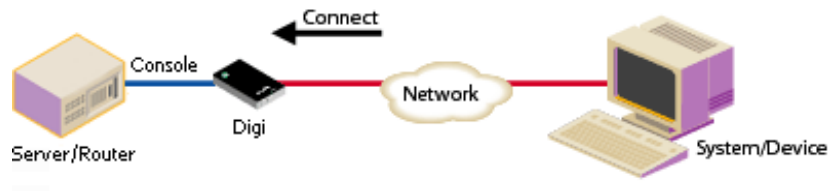


Data is routed to the serial device connected to the Digi Connect Family device's serial port. The network is transparent to both the application and the serial device.

Important: On each PC that will use RealPort ports, RealPort software must be installed from the Software and Documentation CD. and configured. Enter the IP address of the Digi Connect Family device and the RealPort TCP port number 771.

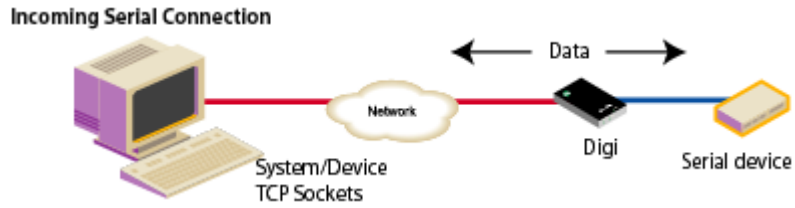
Console Management Profile

The Console Management Profile allows access to a device's console port over a network connection. Most network devices such as routers, switches, and servers offer serial port(s) for management. Instead of connecting a terminal to the console port, cable the console port to the serial port of your Digi Connect Family device. Then using Telnet features, network administrators can access these consoled serial ports from the LAN by addressing the appropriate TCP port.



TCP Sockets Profile

The TCP Sockets profile allows serial devices to communicate over a TCP network. The TCP Server allows other network devices to initiate a TCP connection to the serial device attached to the serial port of the Digi Connect Family device.



Automatic TCP Connections (Autoconnection)

The TCP Client allows the Digi Connect Family device to automatically establish a TCP connection to an application or a network, known as autoconnection. Autoconnection is enabled through the TCP Sockets profile's setting labeled **Automatically establish TCP connections**.

RFC 2217 Support

Digi Connect Family devices support RFC 2217, an extension of the Telnet protocol used to access serial devices over the network. RFC 2217 implementations enable applications to set the parameters of remote serial ports (baud rate, flow control, etc.), detect line signal changes, as well as receive and transmit data. The configuration information provided in this section applies to Digi Connect Family devices functioning as RFC 2217 servers.

If using the RFC 2217 protocol, do not modify the port settings from the defaults. If the port settings have been changed, restore the factory default settings (see "Restore a Device Configuration to Factory Defaults" on page 160). No additional configuration is required.

TCP and UDP Network Port Numbering Conventions

Digi Connect Family devices use these conventions for TCP and UDP network port numbering.

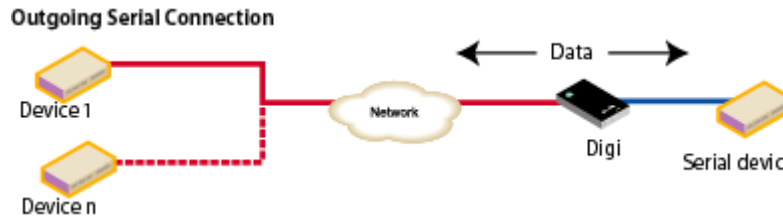
For this connection type...	Use this Port
Telnet to the serial port	2001 (TCP only)
Raw connection to the serial port	2101(TCP and UDP)

Ensure that the application or device that initiates communication with the Digi Connect Family device uses these network ports numbers. If they cannot be configured to use these network port numbers, change the network port on the Digi Connect Family device.

UDP Sockets Profile

The UDP Sockets profile allows serial devices to communicate using UDP. The UDP Server configuration allows the serial port to receive data from one or more systems or devices on the network. The UDP Client configuration allows the automatic distribution of serial data from one host to many devices at the same time using UDP sockets.

The port numbering conventions shown in the TCP Sockets Profile also apply to UDP sockets.



Serial Bridge Profile

The Serial Bridge profile configures one side of a *serial bridge*. A serial bridge connects two serial devices over the network, each of which uses a Digi device, as if they were connected with a serial cable. The serial devices "think" they are communicating with each other across a serial cable using serial communication techniques. There is no need to reconfigure the server or the serial device. Neither is aware of the intervening network. Serial bridging is also known as *serial tunneling*.

This profile configures each side of the bridge separately. Repeat the configuration for the second Digi device of the bridge, specifying the IP address of the first Digi device.

Local Configuration Profile

The Local Configuration profile allows for connecting standard terminals or terminal emulation programs to the serial port in order to use the serial port as a console to access the command line interface. Profile settings enable and disable access to the command line.

Modem Emulation Profile

The Modem Emulation profile allows Digi Connect Family family to emulate a modem. It sends and receives modem responses to the serial device over the Ethernet instead of PSTN (Public Switched Telephone Network). This profile allows maintaining the current software application but using it over a less-expensive Ethernet network.

The commands that can be issued in a modem-emulation configuration are described in the *Digi Connect Family Command Reference*.

Custom Profile

The Custom port profile displays all serial-port settings, which can be changed as needed. Use the Custom profile only if the use of the serial port does not fit into any of the predefined port profiles, for example, if network connections involve a mix of TCP and UDP sockets.

Basic Serial Settings

After selecting a port profile, the profile settings are displayed. Choose the appropriate features for your environment. Here are brief descriptions of the fields in the Basic Serial Settings; see the online help for detailed information about each setting.

- The **Description** field specifies an optional character string for the port which can be used to identify the device connected to the port.
- **Basic Serial Settings** include **Baud Rate**, **Data Bits**, **Parity**, **Stop Bits**, and **Flow Control**. The basic serial port settings must match the serial settings of the connected device. If you do not know these settings, consult the documentation that came with your serial device. These serial settings may be documented as 9600 8N1, which means that the device is using a baud rate of 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

  When using RealPort (COM port redirection) or RFC 2217, these settings are supplied by applications running on the PC or server, and the default values on your Digi Connect Family device do not need to be changed.

Advanced Serial Settings

The advanced serial settings allow you to further define the serial interface, including whether port buffering (also known as port logging), RTS Toggle, and RCI over Serial are enabled as general serial interface options. You can also define how specific aspects of TCP and UDP serial communications should operate, including timeouts and whether a socket ID is sent.

Serial Settings

The **Serial Settings** part of the page includes these options:

- **Enable Port Logging:** Enables the port-buffering feature, which allows you to monitor incoming ASCII serial data in log form. The Log Size field specifies the size of the buffer that contains the log of ASCII serial data.
- **Enable RTS Toggle:** When enabled, the RTS (Request To Send) signal is forced high (on) when sending data on the serial port.
- **Enable RCI over Serial (DSR):** This choice allows the Digi Connect device to be configured through the serial port using the RCI protocol. See the RCI specification in the Digi Connect Integration Kit for further details.

  RCI over Serial uses the DSR (Data Set Ready) serial signal. Verify that the serial port is not configured for autoconnect, modem emulation, or any other application which is dependent on DSR state changes.

TCP Settings

The **TCP Settings** are displayed only when the current serial port is configured with the TCP Sockets or the Custom Profile. The settings are as follows:

- **Send Socket ID:** Include an optional identifier string with the data sent over the network. The Socket ID can be 1 to 256 ASCII characters. To enter non-printable characters, use these key sequences:

Character	Key Sequence
backspace	\b
formfeed	\f
tab	\t
new line	\n
return	\r
backslash	\\
hexadecimal values	\xhh

- **Send data only under any of the following conditions:** Enable if it is required to set conditions on whether the Digi Connect Family device sends the data read from the serial port to the TCP destination. Conditions include:
  - **Send when data is present on the serial line:** Send the data to the network destinations when a specific string of characters is detected in the serial data. Enter the string 1 to 4 characters in the Match String field. To enter non-printable characters, use these key sequences:

Character	Key Sequence
hexadecimal values	\xhh
tab	\t
line feed	\n
backslash	\\

  - **Strip match string before sending:** Match string before sending to strip the string from the data before it is sent to the destination.
  - **Send after the following number of idle:** Send the data after the specified number of milliseconds has passed with no additional data received on the serial port. This can be 1 to 65,535 milliseconds.
  - **Send after the following number of bytes:** Send the data after the specified number of bytes has been received on the serial port. This can be 1 to 65,535 bytes.
- **Close connection after the following number of idle seconds:** Enable to close an idle connection. Use the Timeout field to enter the number of seconds that the connection will be idle before it is closed. This can be 1 to 65000 seconds.
- **Close connection when DCD goes low:** When selected, the connection will be closed when the DCD (Data Carrier Detected) signal goes low.
- **Close connection when DSR goes low:** When selected, the connection will be closed when the DSR (Data Set Ready) signal goes low.

UDP Settings

The UDP Settings are displayed only when the current serial port is configured with the UDP Sockets or the Custom Profile.

- **Send Socket ID:** Include an optional identifier string with the data sent over the network. The Socket ID can be 1 to 256 ASCII characters. To enter non-printable characters, use these key sequences:

Character	Key Sequence
backspace	\b
formfeed	\f
tab	\t
new line	\n
return	\r
backslash	\\
hexadecimal values	\xhh

Configure GPIO Pins

All Digi Connect devices except the Digi Connect SP and Digi Connect Wi-SP have several General Purpose IO (GPIO) pins. In normal operation, the GPIO pins are used for the serial CTS, DCD, DSR, DTR, and RTS signals. On Digi Connect EM and Wi-EM products, both sets of RXD/TXD signals are also configured. These GPIO pins can be used for either standard serial communication signalling or for a user-defined purpose, such as when a significant event occurs within the device. In the latter case, the Digi device can be configured so that when an event occurs, an alarm can be sent in the form of an email message to an administrator or technician, or in the form of an SNMP trap.

The number of GPIO pins varies by device. Digi Connect ME and Wi-ME devices have five GPIO pins, while Digi Connect EM and Wi-EM devices have nine GPIO pins.

The configuration and current state of GPIO pins can be easily viewed, through the Web user interface or by issuing commands from the command line.

GPIO Pin Settings

The GPIO Configuration page configures the GPIO pin settings. GPIO pins can be configured for one of three modes: serial, input, and output.

- **Serial:** The GPIO pin is used for standard or normal serial communication signalling. Each pin maps to a different serial signal: DCD, CTS, DSR, etc. Here are default serial settings for the GPIO pins on a Digi Connect Family device. Depending on the device, there are five or nine pins.

Pin Number	Default Serial Signal	Signal Direction
GPIO 1	DCD	Input
GPIO 2	CTS	Input
GPIO 3	DSR	Input
GPIO 4	RTS	Output
GPIO 5	DTR	Output
GPIO 6	TXD	Output
GPIO 7	RXD	Input
GPIO 8	TXD for port 2	Output
GPIO 9	RXD for port 2	Input

- **In:** Allows input of GPIO signals. The GPIO pin is used for user-defined signal input from the connected device to the Digi Connect Family device. Alarms can be issued when GPIO pins change state. Input mode is used in with alarms to trigger email notifications or SNMP traps when a particular signal change is detected, as discussed in "Configure Alarms" on page 104.
- **Input mode**: allows input of GPIO signals.
- **Out:** Allows output of GPIO signals. The GPIO pin is used for user-defined signal output from the Digi Connect Family device to the connected device. This mode can be used to toggle the output of GPIO signals between high and low.

Additional Implementation Required for Input and Output Choices

Changing the GPIO pin settings from Serial to Input or Output means you are responsible for implementing how the pins and signals will work, including developing any applications, signal-handling, and hardware.

Set Alarms for GPIO Pin Changes, as Needed

To issue alarms in the form of email notifications or SNMP traps when a GPIO pin signals that an event has occurred on the Digi Connect Family device, go to the Alarms page and configure those alarms. See "Configure Alarms" on page 104.

Test GPIO Pins

Once the GPIO pins and any alarms associated with them have been configured, test the GPIO pins to make sure they work as desired.

Test GPIO Input

Typically, input signals on GPIO pins are used to trigger an email alarm, which tells an administrator or technician that a significant event has occurred within the device. The process for testing GPIO input is as follows:

1. On the SW2 bank of switches on the development board, ensure that one of the GPIO pins is set to High.
2. On the SW1 bank of switches, set the same GPIO pin to IO.
3. Configure the GPIO pin for input. See "Configure GPIO Pins" on page 100.
4. Configure an email alarm for the GPIO pin. See "Configure Alarms" on page 104.
5. Toggle the SW2 switch several times to generate several email alarms.

Test GPIO Output

The process for testing GPIO output is as follows. In this process, raising a GPIO signal from the configuration application causes an LED on the development board to turn on.

1. On the SW2 bank of switches on the development board, ensure that one of the GPIO pins is set to High.
2. On the SW1 bank of switches, set the same GPIO pin to IO.
3. In the Web user interface for the Digi Connect device, click the GPIO link. On the GPIO page, configure one or more GPIO pins for output. See "Configure GPIO Pins" on page 100 for details.
4. Under Administration, click the System Information link. On the System Information page, click the GPIO link.
5. Choose Asserted to raise the signal, and then click Set Pins.

   An LED on the development board is turned on.

   Note that this process does not configure the Digi Connect device. Settings are not saved. If the module reboots, perform steps 2 and 3 again.

Configure Alarms

Use the Alarms page to configure device alarms or display current alarms settings. Device alarms are used to send email messages or SNMP traps when certain device events occur. These events include changes in GPIO signals, certain data patterns being detected in the data stream.

Alarm Notification Settings

On the Alarms page, the Alarm Notification Settings control the following:

- **Enable alarm notifications:** Enables or disables all alarm processing for the Digi Connect device.
- **Mail Server Address (SMTP):** Specifies the IP address of the SMTP mail server. Ask your network administrator for this IP address.
- **From:** Specifies the text that will be used in the “From:” field for all alarms that are sent as emails.

Alarm Conditions

The Alarm Conditions part of the Alarms page shows a list of all of the alarms. Up to 32 alarms can be configured for a Digi Connect Family device, and they can be enabled and disabled individually.

Alarm List

The list of alarms displays the current status of each alarm. If there are any alarms already configured for the device, and after configuring any new alarms, this list can be used to list to view alarm status at a glance, then view more details for each alarm as needed.

- **Enable:** Checkbox indicates whether the alarm is currently enabled or disabled.
- **Alarm:** The number of the alarm.
- **Status:** The current status of the alarm, which is either enabled or disabled.
- **Type:** Specifies whether the alarm is based on GPIO pin state changes or serial data pattern matching.
- **Trigger:** The conditions that trigger the alarm.
- **SNMP Trap:** Indicates whether the alarm is sent as an SNMP trap.
  - If the SNMP Trap field is disabled, and the Send To field has a value, then the alarm is sent as an email message only.
  - If the SNMP trap field is enabled and the Send To field is blank, then the alarm is sent as an SNMP trap only.
  - If the SNMP Trap field is enabled, and a value is specified in the Send to field, then that means the alarm is sent both as an email and as an SNMP trap.
- **Send To:** The email address to which the alarm is sent.
- **Email Subject:** The text to be included in the “Subject:” line of any alarms sent as email messages.

Alarm Conditions

To configure an alarm, click on it. The configuration page for individual alarms has two sections:

- **Alarm Conditions:** For specifying the conditions on which the alarm is based, such as GPIO pin state changes, serial data pattern matching, signal strength (RSSI), or data usage.
- **Alarm Destinations:** For specifying how the alarm is sent, either as an email message or an SNMP trap, or both, and where the alarm is sent.

Alarm Conditions

The Alarm Conditions part of the page is for specifying the conditions on which the alarm is based. Alarm conditions include:

- **Send alarms based on GPIO pin states:** Click this radio button to specify that this alarm is sent when the specified GPIO pin states are detected. Then specify the following:
  - **Pins:** An alarm is sent when the specified combination of pin states is detected.

    High - pin is asserted.

    Low - pin is not asserted.

    Ignore - pin state is ignored.
  - **Alarm recurrence time:** Defines how often a new alarm can be sent. For example, if the alarm recurrence time is 10 seconds then even if the pin states are detected 5 times within a 10 second period only one alarm will be sent.
  - **Send reminders while GPIO pins remain in this state:** If enabled, reminders will be sent if the pins remain in the defined state for an extended period of time.
  - **Every:** The number of seconds the pins must remain in the defined state for a reminder to be sent.
- **Send alarms based on serial data pattern matching:** Click this radio button to specify that this alarm is sent when the specified serial data pattern is detected. Then specify the following:
  - **Serial Port:** The serial port to monitor for the data pattern. This field is displayed for devices where more than one serial port is available.

- **Pattern:** An alarm is sent when the serial port receives this data pattern. Special characters such as carriage return carriage return (\r) and new line (\n) in the data pattern can be included.

Alarm Destinations

The Alarm Destination part of the page defines how alarm notifications are sent—either as an email message or an SNMP trap, or both—and where the alarm notification is sent.

- **Send E-mail to the following recipients when alarm occurs:** Select the checkbox to specify that the alarm should be sent as an email message. Then specify the following information:
  - **To:** The email address to which this alarm notification email message will be sent.
  - **CC:** The email address to which a copy of this alarm notification email message will be sent (optional).
  - **Priority:** The priority of the alarm notification email message.
  - **Subject:** The text to be included in the Subject: line of the alarm-notification email message.
- **Send SNMP trap to the following destination when alarm occurs:** Select the checkbox to specify that the alarm should be sent as an SNMP trap.

  For alarms to be sent as SNMP traps, the IP address of the destination for the SNMP traps must be specified in the SNMP settings. This is done on the System Configuration pages of the Web user interface. See "SNMP Configuration Settings" on page 108. That destination IP address is then displayed below the “Send alarm to SNMP destination” checkbox.
- To configure an alarm notification to be sent as both an email message and an SNMP trap, select both **Send E-Mail** and **Send SNMP trap** checkboxes.
- Click **Apply** to apply changes for the alarm and return to the Alarms Configuration page.

Enable and Disable Alarms

Once alarm conditions are configured, enable and disable individual alarms by selecting or deselecting the Enable checkbox for each alarm.

Configure System Settings

The System Configuration page configures system settings, including device description information, such as the device name, contact, and location, and whether SNMP is enabled or disabled and the SNMP traps that are enabled.

Device Description Information

A device description is a system description of the Digi Connect Family device's name, contact, and location. This device description can be useful for identifying a specific Digi Connect Family device when working with a large number of devices in multiple locations.

SNMP Configuration Settings

Simple Network Management Protocol (SNMP) is a protocol that can be used to manage and monitor network devices. Digi Connect Family devices can be configured to use SNMP features, or SNMP can be disabled entirely for security reasons. To configure SNMP settings, click the **Simple Network Management Protocol** link at the bottom of the System Configuration page. SNMP settings include:

- **Enable Simple Network Management Protocol (SNMP):** This checkbox enables or disables use of SNMP.
- 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 is recommended to prevent unauthorized access to the device.
  - Public community: The password required to get SNMP-managed objects. The default is **public**.
  - Private community: The password required to set SNMP-managed objects. The default is **private**.
- **Allow SNMP clients to set device settings through SNMP:** This checkbox enables or disables the capability for users to issue SNMP "set" commands uses use of SNMP read-only for the Digi Connect Family device.
- **Enable Simple Network Management Protocol (SNMP) traps:** Enables or disables the generation of SNMP traps.
- **Destination IP:** The IP address of the system to which traps are sent. In order to enable any of the traps, a non-zero value must be specified. For Digi Connect

products that support alarms, this field is required in order for alarms to be sent in the form of SNMP traps. See "Configure Alarms" on page 104.

- At the bottom of the page are checkboxes for the SNMP traps that can be used: authentication failure, login, cold start, and link up traps.

Configure Remote Management (Connectware Manager Settings)

The Remote Management configuration page sets up the connection to the Connectware Manager server so the Digi Connect Family device knows how to connect to the server.

The Connectware Manager server allows devices to be configured and managed from remote locations.

Procedure for Setting Up Remote Management

Using Connectware Manager as a remote manager of a Digi Connect Family device requires several steps:

1. Install The Connectware Manager server on a server system. See the *Connectware Manager Getting Started Guide* for installation instructions
2. Assign a device ID defined for the Digi Connect Familydevice. See the *Connectware Manager Operator's Guide's* instructions for adding a device.

   Important: The device ID for the Digi Connect Family device must be unique. By default, the device ID is created from the MAC address of the device.
3. From the Web user interface, configure the Remote Management settings so the device can communicate with the Connectware Manager server.

   There are two pages of remote management settings: Connections and Advanced settings.

Connection Settings

The Connection settings configure how the Digi device connects to the Connectware Manager server. These settings include information about communication between client and server and the connection methods used by the various interfaces on the system.

About Client-initiated and Server-initiated Connections

Digi Connect Family devices can be configured to connect to and communicate with the Connectware Manager server through client-initiated or server-initiated connections.

In a *client-initiated connection*, the Digi Connect Family device attempts to connect to the network, and will continue attempts to reach the Connectware Manager server to establish the connection. To maintain the connection, the Digi Connect Family device sends *keep-alive messages* over the connection. The frequency with which keep-alive messages are sent is configurable. An advantage of client-initiated connections is that they can be used in any cellular network, whether public or private IP addresses are used, or even if NAT is used. A disadvantage is that you can be charged for the Digi Connect Family device sending the keep-alives, depending on your cellular/mobile service plan.

A *server-initiated connection* works the opposite way. The Connectware Manager server opens a TCP connection, and the Digi Connect Family device must be listening for the connection to the Connectware Manager server to occur. An advantage of server-initiated connections is that you are not charged for sending the keep-alive bytes that are used in client-initiated connections. A disadvantage is that there is no way of knowing whether the devices displayed in the device list at the Connectware Manager server are offline or connected. The device list shows all the devices as disconnected until the Connectware Manager server does something to interact with them. In addition, server-initiated connections cannot be used if Digi Connect Family devices have private IP addresses and are behind a NAT.

Last Known Address (LKA)

Changes to the IP address for a Digi Connect Family device present a challenge in server-initiated connections, because the Connectware Manager server needs to locate the Digi Connect Family device by its new IP address. Digi Cellular Family devices handle address changes by sending a Last Known Address (LKA) update to the Connectware Manager server. This permits the Connectware Manager to connect back to the Digi Connect Family device, or to dynamically update a DNS with the IP address of the device.

Client Initiated Management Connection Settings

- **Enable Remote Management and Configuration using a client initiated connection:** Configures the connection to the Connectware Manager server to be initiated by the Connectware Manager client, that is, this Digi Connect Family device.
- **Server Hostname:** The IP address or hostname of the Connectware Manager server.
- **Automatically reconnect to the server after being disconnected**
  Wait for: Whether to automatically reconnect to the server after being disconnected and waiting for the specified amount of time.

Server Initiated Management Connection Settings

- **Enable Remote Management and Configuration using a server initiated connection:** Configures the connection to the Connectware Manager server to be initiated by the Connectware Manager server.
- **Enable Last Known Address (LKA) updates to the following server:** Enables or disables a connection to a Connectware Manager server to inform that server of the IP address of the Digi Connect Family device, known as a "last known address" (LKA) update. This permits the Connectware Manager to connect back to the Digi Cellular Family device, or to dynamically update a DNS with the IP address of the device.
- **Server Hostname:** The IP address or hostname of the Connectware Manager server.
- **Retry if the LKA update fails:**
  Retry every: These options specify whether another "last known address" update attempt should be made after a previous attempt failed, and how often the retry attempts should occur.

Advanced Remote Management Settings

The default settings for remote management usually work for most situations. These Advanced settings are used in advanced situations. They are used to configure the idle timeout for the connection between the Digi Connect Family device and the Connectware Manager server, and the keep-alive settings of the various interfaces (TCP and HTTP Ethernet network connections). These settings should only be changed when the defaults do not properly work.

- **Connection Settings:** These settings configure the idle timeout for the connection between the Digi Connect Family device and the Connectware Manager server.
  - **Disconnect when Connectware Management is idle:** Enables or disables the idle timeout for the connection. If enabled, the connection will be dropped, or ended, after the amount of time specified in the **Idle Timeout** setting.
  - **Idle Timeout:** The amount of time to wait before timing out the connection.
- **Ethernet Settings:** These settings apply to client-initiated management connections over the Ethernet network.
  - **Connectware Management Protocol Keep-Alive Settings:** These settings control how often keep-alive packets are sent over the client-initiated connection to the Connectware Manager server, and whether the device waits before dropping the connection.

    Receive Interval: The number of seconds to wait for a keep-alive message from the Connectware Manager server before assuming the connection is lost.

    Transmit Interval: The number of seconds to wait between sending keep-alive messages. (

    Assume connection is lost after *n* timeouts: How many timeouts occur before the Digi Connect Family device assumes the connection to the Connectware Manager server is lost and drops the connection.

– **Connection Method:** The method for connecting to the Connectware Manager server.

  TCP: Connect using TCP. This is the default connection method, and is typically good enough for most connections. It is the most efficient method of connecting to the remote server in terms of speed and transmitted data bytes.

  Automatic: Automatically detect the connection method. This connection method is less efficient than TCP, but it is useful in situations where a firewall or proxy may prevent direct connection via TCP. Automatic will try each combination until a connection is made. This connection method requires the HTTP over Proxy Settings to be specified.

  None: This value has the same effect as selecting TCP.

  HTTP: Connect using HTTP.

  HTTP over Proxy: Connect using HTTP.

– **HTTP over Proxy Settings:** The settings required to communicate over a proxy network using HTTP. These settings apply when **Automatic** or **HTTP over Proxy** connection methods are selected.

  Hostname: The name of the proxy host.

  TCP Port: The network port number for the TCP network service on the proxy host.

  Username:
  Password: The username and password for logging on to the proxy host.

  Enable persistent proxy connections: Specifies whether the Digi Connect Family device should attempt to use HTTP persistent connections. Not all HTTP proxies correctly handle HTTP persistent connections. The use of persistent connections can improve performance of the exchange of messages between the device server and Connectware Manager, when that connection is HTTP/proxy. The reason for this is that the same HTTP connection can be reused for multiple consecutive HTTP requests and replies, eliminating the overhead of establishing a new TCP connection for each individual HTTP request/reply, then closing that connection when the request is complete.

Alarms and the Connectware Manager Server

All alarms can be sent to the Connectware Manager server for display and management from that interface. See "Configure Alarms" on page 104.

For More Information on Connectware Manager

The *Connectware Manager Operator's Guide* provides detailed information on Connectware Manager features and tasks performed from the Connectware Manager console.

Configure User Settings

User settings involve several areas:

- **User authentication:** whether authentication is required for users accessing the Digi Connect Family device, and the information required to access it. Depending on the Digi product, multiple users and their authentication information can be defined. User authentication settings are on the Users settings page.
- **User access settings:** the device interfaces that a user can access, such as the command line or Web user interface.
- **User permissions settings:** the permissions a user has to access and configure the Digi Connect device.
- Several settings on the Network Configuration pages are available to further secure the Digi Connect Family device. For example, on the **Network Services** page, you can disable unused network services.

About User Models and User Permissions

Several user models are implemented in the Digi Connect Family products:

- Two-user model
- More than two-user model

To determine which user model is implemented:

- In the Web user interface, if the menu includes **Users**, the Digi Connect device uses either the two-user model or the more than two users model.
- In the command-line interface, issue a **show user** or **set user** command. In the command output, note how many user IDs are defined: one, two, or more than two. Or, issue a **set user ?** command and note the range for the **id=*range*** option. If the **id=** option is not listed, there is only one user. Otherwise, the range for user IDs is displayed. (These commands are described in detail in the *Digi Connect Family Command Reference*.)

Two-User Model

- User 1 has a default name of **root**. This user is also known as the administrative user.
- User 1 has default permissions that enables it to issue all commands.
- Permissions for User 1 can be changed to be less than the default root permissions.
- User 2 is undefined. That is, it does not exist by default, but it can be defined.
- When defined, User 2 has a limited set of permissions, defined by the User Permissions settings in the Web user interface, or the **set permissions** command in the command-line interface (see the **set permissions** command description in the *Digi Connect Family Command Reference*).
- Permissions for User 2 can be changed to be either greater than or less than its default.

Caution Exercise caution in setting permissions for devices that use this user model. A user cannot set another user's permission level higher than their own permission level, nor can a user raise their own permission level.

More than Two-User Model

User definitions are exactly the same as the two-user model, with the addition of user groups and more users. The **set group** command defines user groups (see the **set group** command description in the *Digi Connect Family Command Reference*). Currently, there is no Web user interface page for defining user groups.

Special Feature for Digi Connect ME Only

The Digi Connect ME uses the two-user model, but the login prompt (password authentication) can be disabled.

Password Authentication

By default, Digi Connect Family devices have password authentication enabled. That means when a login prompt is displayed when accessing the device by opening the Web user interface or issuing a **telnet** command.

Disable password authentication

Password authentication can be disabled as needed.

In the Web user interface:

1. On the Main menu, click **Users**.
2. On the **Users Configuration** page, check the **Enable password authentication** check box.
3. Click **Apply**.

From the command line:

Issue a **newpass** command with a zero-length password.

Change the Password for Administrative User

To increase security, change the password for the administrative user from its default. By default, the administrative username is **root**.

Note Record the new password. If the changed password is lost, the Digi device must be reset to the default firmware settings.

In Digi devices with a single-user model, changing the root password also changes the password for Advanced Digi Discovery Protocol (ADDP). In Digi devices with the multi-user model, changing the root password has no effect on ADDP. To change the ADDP password, use enter **newpass name=addp** from the command line.

In the Web user interface:

1. On the Main menu, click **Users**.
2. On the **Users Configuration** page, click **root**.
3. Enter the new password in the New **Password** and **Confirm Password** edit boxes. The password can be from 4 through 16 characters long and is case-sensitive. Click **Apply**.
4. A logoff is forced immediately. Log in to the Web user interface using the new values.

From the command line:

Issue the **newpass** command.

Add Users

Digi Connect Family products allow multiple users to be defined. For those products, the **Users Configuration** page shows the currently defined users and allows you to add more user definitions. To add a user definition:

1. On the Main menu, click **Users**.
2. On the **Users Configuration** page, click **New**.
3. On the **Add New Users** page, specify the user name and password to be used for login. The password can be from 4 through 16 characters long and is case-sensitive. Confirm the password, and click **Apply**. The changes take effect immediately. No logout/login is necessary.

User Access Settings

For Digi Connect products with the two-user or more-than-two-users model, user access to the device interfaces is configurable. For example, the administrative user can access both the command line and Web user interface, but other users can be restricted to the Web user interface only.

Take care in changing access settings. If you are logged in as the administrative user and disable Web user interface, you will not be able to log in to the Digi Connect device on your next attempt, and there is no way to raise your user permissions to enable the Web user interface again. You must reset the device to factory defaults to enable the Web user interface access.

To set access settings:

1 On the Main menu, click **Users**.

2 On the Users Configuration page's list of users, click on the user.

3 On the User Access page, enable or disable the device interface access as desired:

- **Allow command line access:** Enables or disables access to the command line.
- **Allow web interface access:** Enables or disables access to the Web user interface.

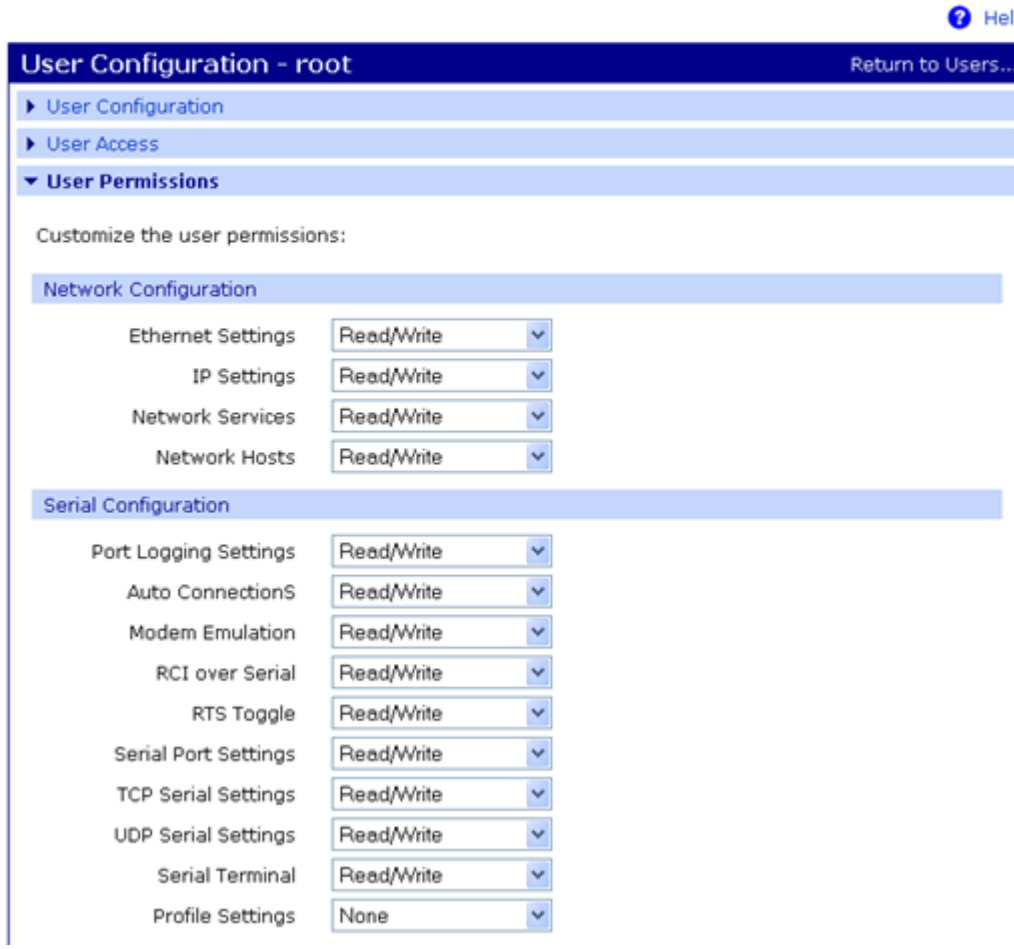
4 Click **Apply**. The changes take effect immediately. No logout/login is necessary.

User Permissions Settings

The User Permissions page is used to define whether and how users can use services and and configuration settings for the Digi Connect product. For example, you can disable a user's access to certain parts of the Web user interface, or allow them to display settings only but not change them.

The list of services and the user permissions available for them vary by Digi Connect product and the features supported in the product.There are several groups of services, such as Network Configuration, Serial Configuration, System Configuration, Command Line Applications, and System Administration, with user permissions for various features. For example here are the Network Configuration and Serial Configuration user permissions for Digi Connect ME:

Digi Connect ME Configuration and Management



User Permissions and Effects

Permission Setting	Effect
None	The user will not have permission to execute this setting.
Read Self	The user will be able to display their own settings, but not those of other users.
Read	The user has permission to read the setting for all users, but does not have permission to modify or write the setting.
Read/Write Self	The user has permission to read and write their own setting, but not those of other users.
Read All/Write Self	The user has permission to read the setting for all users and can modify their own setting.
Read/Write	The user has full permission to read and write the setting for all users.
Execute	The user has full permission to execute this setting.

Restrictions on Setting User Permissions

A user cannot set another user's permission level higher than their own permission level, nor can a user raise their own permission level.

Set User Permissions from the Web User Interface

1. On the Main menu, click **Users**.
2. On the Users Configuration page's list of users, click on the user.
3. Click on **User Permissions**.
4. A list of feature groupings and the user permissions for them is displayed. Customize these settings as needed.
5. Click **Apply**.

Set User Permissions from the Command-Line Interface

User permissions can be set from the command-line interface by the **set permissions** command. See the *Digi Connect Family Command Reference* for the command description.

Disable Unused and Non-Secure Network Services

To further secure the Digi Connect Family device, network services not necessary to the device, particularly non-secure or un-encrypted network services such as Telnet, can be disabled. See "Network Services Settings" on page 84.

Configure Applications

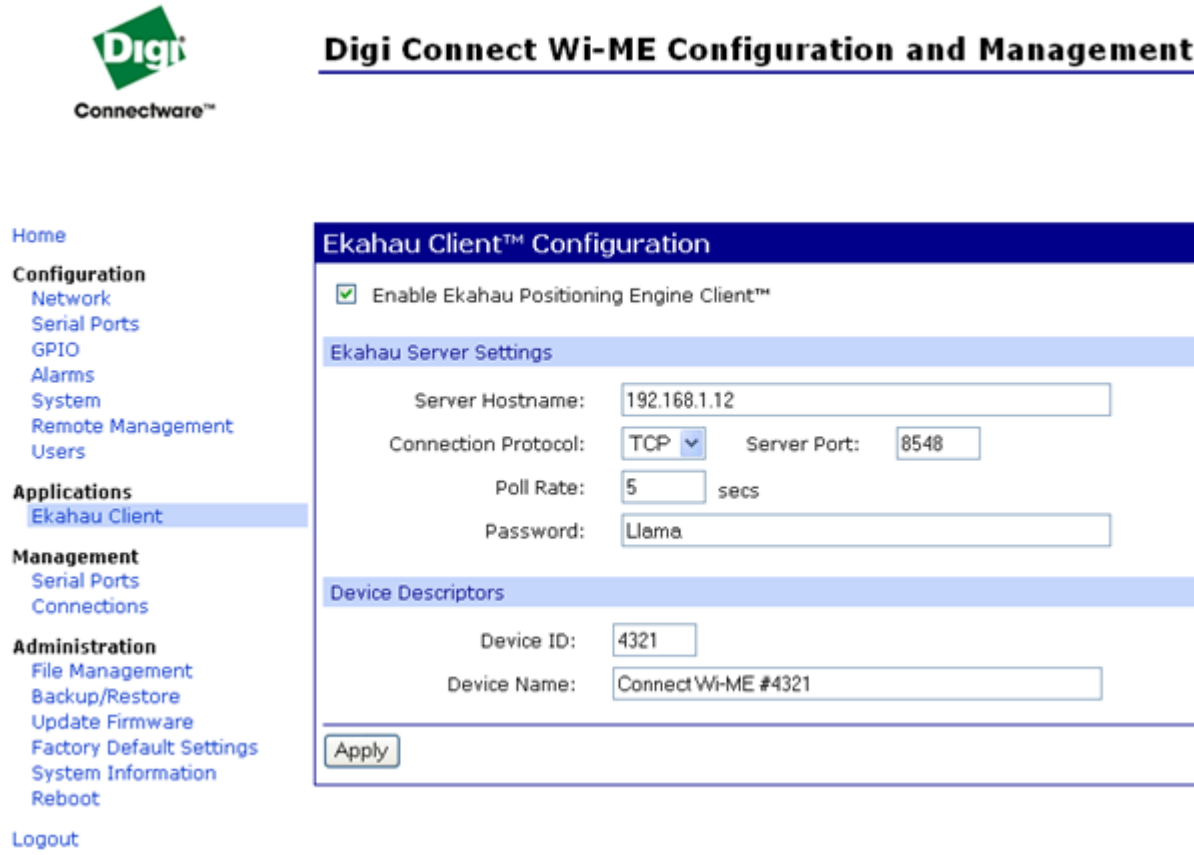
Several Digi Connect products support additional configurable applications. For most devices, these applications are accessed from the main menu under **Applications**. Some devices have an **Applications** link under **Configuration**.

Configure Ekahau Client™

For Digi Connect wireless products, clicking **Ekahau Client** displays a page for configuring Ekahau Client device-location software.

The Ekahau Client feature provides integrated support for Ekahau's Wi-Fi device-location solution, called the Ekahau Positioning Engine, on the Digi Connect Wi-ME, Digi Connect Wi-EM, and Digi Connect Wi-SP products. Ekahau offers a complete access point vendor-independent real-time location system for wireless LAN devices that is capable of pinpointing wireless LAN devices such as the Digi Connect products, laptops, PDAs, or other intelligent Wi-Fi enabled devices. The solution provides floor-, room- and door-level accuracy of up to 3.5 feet (1 m). The patented Ekahau positioning technology is based on simple signal-strength calibration maps, and enables customers to fully leverage an existing wireless LAN infrastructure without any need for proprietary hardware components.

Please visit **www.ekahau.com** for additional information, including free evaluation licenses for the Ekahau Positioning Engine and Ekahau Site Survey software products.



Ekahau Client configuration settings include:

- **Enable Ekahau Positioning Engine Client™:** Enables or disables the Ekahau Positioning Engine Client feature.
  - **Ekahau Server Settings:** Configures how the Ekahau Positioning Engine Client communicates with the server.
  - **Server Hostname:** The hostname or IP address of the Ekahau Positioning Engine. The maximum length of this option is 50 characters. The default is 8548.
  - **Connection Protocol:** Specifies whether to use TCP or UDP as the network transport. The default is TCP.
  - **Server Port:** The network port to communicate on. In the default Ekahau configuration, port 8548 is used for TCP, and port 8549 for UDP.

- **Poll Rate:** The time in seconds between each scan or wireless access points and communication with the server. Once the Ekahau Client is enabled, every time the Digi Connect device scans the network, it is essentially disassociated with the access point (AP) providing its network connectivity. In addition, during the time, or scanning interval, set by the poll rate, it will not be receiving or transmitting wireless packets. This could lead to packet loss. Set the poll rate as slow as acceptable in the application where the Digi Connect product is being used. The default is five seconds.
- **Password:** A password to authenticate with the server. The maximum length of this option is 50 characters. The default for Digi and the Ekahau Positioning Engine is 'Llama'.

■ **Device Descriptors:**

- **Device ID:** A numeric identifier for the Digi Connect device, used internally by the Ekahau Positioning Engine for device tracking over time. This identifier should be unique for each Digi device being located on the network.
- **Device Name:** A descriptive name to identify the Digi Connect device to users. The maximum length of this option is 50 characters.

Alternative Configuration Options for Digi Connect Wi-SP

If configuring the Digi Connect Wi-SP with a serial connection, there are several configuration options.

Configure with an Access Point - Infrastructure Mode

1 Configure the network using an access point with the SSID - Connect and all encryption disabled (such as WEP & WPA).

2 Power up the device.

3 Launch the Discovery program and proceed with the configuration.

Configure without an Access Point - Laptop with a Wireless Card Ad-Hoc Mode

1 Configure the wireless card to operate in Ad-Hoc mode with the SSID - Connect.

2 Power up the device.

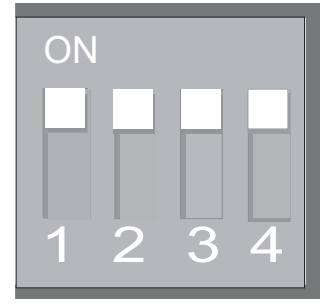
3 Launch the Discovery application on the laptop and proceed with the configuration.

Command Line Access

Note To set the DIP switches on the Digi Connect Wi-SP (or SP), ALWAYS disconnect the power supply before resetting the switches. See the following procedure for more details.

1 Disconnect the power supply.

2 Set the Digi Connect Wi-SP DIP switches in the On or up position. The figure shows DIP Switch settings for Command Line access for both the Digi Connect Wi-SP and the Digi Connect SP.



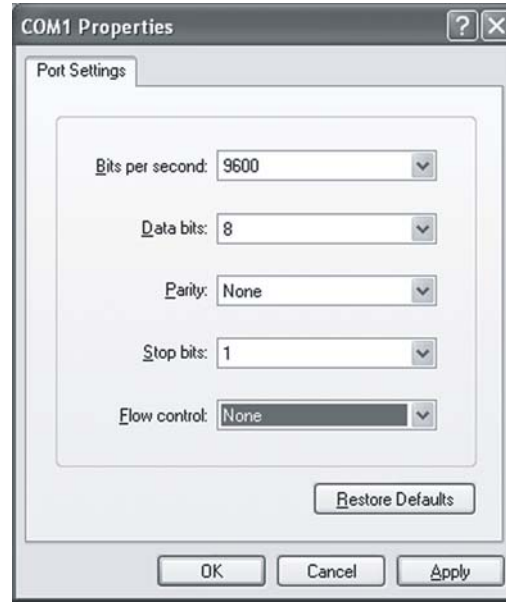
3 Connect the Digi Connect Wi-SP to a PC with a serial cable.

4 Access a terminal emulation program such as HyperTerm.

Choose **Start > Accessories > Communication > Hyperterm** and enter a name for the connection.

5 Select COM1 and click **OK**.

6 Set the port settings to 9600, 8, None, 1, None (default settings) click Apply then OK.



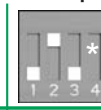
7 Enter the login username: **root**

and the default password: **dbps**

8 Go to the *Digi Connect Family Command Reference* on the Software and Documentation CD for command descriptions. See the **set wlan** command for all parameters.

9 After configuring the Digi Connect Wi-SP parameters to function within your network, disconnect the power supply and the serial cable from the Digi Connect Wi-SP.

10 Reset the DIP switch settings according to serial device requirements (EIA-232/422/485).

		EIA-232	EIA-422/485 Full-Duplex	EIA-485 Half-Duplex
Switch Settings	Up/On Down/Off			
DB-9 Pinouts	1	DCD	CTS-	Not Used
	2	RxD	RxD+	RxD+
	3	TxD	TxD+	TxD+
	4	DTR	RTS-	Not Used
	5	GND	GND	GND
	6	DSR	RxD-	RxD-
	7	RTS	RTS+	Not Used
	8	CTS	CTS+	Not Used
	9	RI	TxD-	TxD-
	Shell	GND		

*If switch 4 is up, termination resistor connected
If down, termination resistor not connected.

11 Connect the antenna and the power supply to the Digi Connect Wi-SP.

12 Insert the Software & Documentation CD and follow the wizard to discover and the configure the Digi Connect Wi-SP for your network.

Note See also Digi support site at **http://www.digi.com/support/** for additional command resources.

Configuration through the Java Applet Interface

A Java applet interface is available as an alternative device interface.

Accessing the Java Applet Interface

The Java Applet interface can be temporarily launched as a device interface, or can be set as the default interface. In some cases, a system administrator may have already set it as the default.

To launch the Java Applet interface, go to the Home page of the Web user interface. Under **User Interface**, click the **Launch** button to launch the Java applet.

To set the Java applet as the default device interface, click the **Set as Default** button.

Differences Between Web and Java Applet Interfaces

The Java applet interface differs from the Web user interface in these areas:

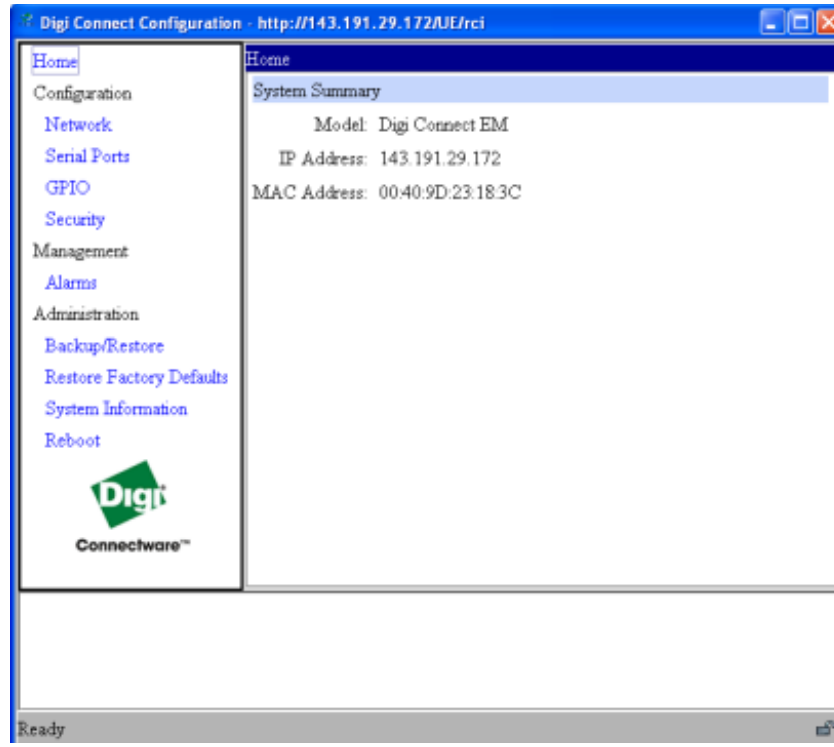
- While the Web user interface runs directly on the device, the Java applet runs remotely. This means when the Java applet launches, all device settings are updated from the device and stored in memory. These are the settings shown when clicking on a configuration choice or clicking **Cancel**.
- Because the Java applet runs remotely, it is not always aware when settings have been changed by other users. Therefore, it is sometimes necessary to refresh the applet to retrieve those settings.
- There are fewer configuration options under **Configuration**: **Network, Serial Ports**, **GPIO**, and **Security**. Alarm configuration is organized under **Management**, and there is no **System** configuration option.
- Some features have limited configuration settings. For example, port profiles are not available in the Serial Ports settings.
- The button for saving configuration settings is labeled **Save** rather than **Apply**, and there are additional buttons: **Cancel** and **Apply**.
- A status pane logs all activities in a session.
- Online help available for the applet screens is limited. As needed, switch to the Web user interface and review the online help for the screens in that interface.

System Requirements

Using the Java applet interface requires that the Sun Java Runtime environment be loaded on the computer used to configure, monitor, and administer the Digi Connect device.

The Home Page

When the Java applet interface for a Digi Connect device is opened, the Home page is displayed.



The left side of the home page has a menu of choices that link to pages for configuration, management, and administration tasks. This section focuses on the links under **Configuration** and **Management**. For details on using the links under **Administration**, see Chapter 4, "Administration Tasks".

The **System Summary** section notes all currently available device-description information.

Configuration Pages

In the menu on the left side of the screen, the choices under **Configuration** are links for configuring various features, including:

- **Network**: Configures network communications. See page 132.
- **Serial Ports**: Configures serial ports. See page 132.
- **GPIO**: Configures the GPIO pins. See page 133.
- **Security**: For configuring security features. See page 133.
- In addition, to configure alarms, use the **Alarms** link under **Management**. See page 133

Some configuration settings are organized on tabs. For example, the **Serial Ports Configuration** screen has tabs for **Basic**, **Port Services**, **Network Services**, and **Advanced** settings.

Saving, Canceling, and Refreshing Configuration Settings

The configuration screens in the Java applet interface contain several buttons: **Save**, **Cancel**, and **Refresh**.

- **Save**: Saves changed values to the Digi Connect device.
- **Cancel**: Resets only those changes that have been made prior to clicking **Save** to the initial values on the particular page. For example, **Cancel** would be useful in the following sequence:

  1. Click on the **Network** choice, and on the **Network** page, DHCP is currently selected.
  2. Instead, select the option to manually assign a static IP.
  3. Next, enter an IP address and Subnet Mask.
  4. Values for those settings are not desired. Click **Cancel**.
  5. The **Network** configuration pages are returned to their initial settings, in which DHCP was selected.

- **Refresh**: Because the Java applet runs remotely, it is not always aware when device settings have been changed by other users. It is sometimes necessary to refresh the applet to retrieve those settings. When the Java applet interface is launched, all device settings are updated and stored in memory. These are the settings that are shown when opening a page of configuration settings or clicking **Cancel**. **Refresh** updates all the stored settings with the settings from the Digi Connect Family device (that is, if someone else had made a change while you were navigating through the applet).

Restoring Settings

There is no way in the Applet or Web UI to restore a certain group of settings to factory defaults. Once settings are saved, they reside in the device. To restore the device to its true default settings, reset the device to factory defaults. See "Restore a Device Configuration to Factory Defaults" on page 160.

Configure Network Settings

To configure network settings, click the **Network** link. Network settings are organized on three tabs:

- **Basic**: Shows how the device's IP address is obtained, either by DHCP or by using a static IP address, subnet mask, and default gateway. Contact your network administrator if you do not know what these settings mean, or when they need to be entered or referenced.
- **Network Services**: Shows a set of common network services that are available for devices, and the port on which the service is running. Network services can be enabled or disabled, and the TCP port on which the network services listen can be changed from the default, with some exceptions. Disabling services may be done for security purposes so that a device is running only those services specifically needed by the device. Any non-secure services, such as Telnet, can be disabled. For a discussion of the effects of disabling these network services, see "Network Services Settings" on page 84
- **Advanced**: Shows advanced network settings, including the Ethernet Interface speed and duplex mode (**Auto**, **Half-Duplex**, or **Full Duplex**).

Configure Serial Ports

To configure serial ports, click **Serial Ports**. In contrast to the Web user interface, the Java applet interface does not make use of port profiles to configure serial port settings. The serial port information is similar to that shown for the Custom Profile in the Web user interface. The **Serial Configuration** page involves several groups of settings arranged on tabs:

- **Basic**: Shows basic serial configuration settings, such as baud rate, data bits, parity, stop bits, and flow control.
- **Port Services**: Configures TCP and UDP client services.
- **Network Services**: Configures services that monitor data on the network and relay it to the serial port.
- **Advanced**: Advanced serial configuration settings for TCP and UDP client services, including whether a socket ID is sent, and whether a connection should be closed after a certain number of idle seconds or if the DCD or DSR signals go low.

Configure GPIO Pins

To configure GPIO pins, click the **GPIO** link. GPIO pin configuration is similar to that in the Web user interface. Current settings for all GPIO pins are shown, and they can be changed as needed. Once GPIO pins are configured, alarms can be defined to send notifications in the event of any changes to GPIO pin states.

Configure Alarms

To configure alarms in the Java Applet interface, go to **Management > Alarms**.

The checkbox at the top of the screen shows whether alarms are currently enabled or disabled.

The **Email Server Information** fields show the IP address of the email server used to send emails when conditions that trigger an alarm occur, and the text to include in the "from" field of an alarm-triggered email.

The **Alarm List** shows all the alarms that are currently defined for a device.

There are several differences for alarm configuration in the Java applet.

Alarms can be configured to be sent as email messages only. They cannot be sent as SNMP traps. The alarm configuration either needs to be overridden by toggling to the default Web UI or by issuing a followup **set alarm** command from the command-line interface.

The method for specifying trigger conditions differs from the one in the Web user interface, where each trigger condition has a combo box for selecting the condition. In the Java applet, conditions are defined by specifying one of the following values:

- X: Ignore
- 1: High
- 0: Low

Configure Security Features

To configure security features, click the **Security** link. Configurable security features are limited to specifying whether password authentication is required for the Digi Connect Family device, and the user name and password required for logging on to the Digi Connect Family device.

Configuration through the Command Line

Configuring a Digi Connect Family device through the command-line interface consists of entering a series of commands to set values in the device. The *Digi Connect Family Command Reference* describes the commands used to configure, monitor, administer, and operate Digi Connect Family devices.

Access the Command Line

To configure devices using commands, first access the command line. Either launch the command-line interface from the last page of the Digi Device Setup Wizard or use the **telnet** command. Enter the **telnet** command from a command prompt on another networked device, such as a server, as follows:

```
#> telnet ip-address
```

where *ip-address* is the IP address of the Digi Connect Family device. For example:

```
#> telnet 192.3.23.5
```

If security is enabled for the Digi Connect Family device, (that is, a username and password have been set up for logging on to it), a login prompt is displayed. If the user name and password for the device are unknown, contact the system administrator who originally configured the device.

Verify Whether Commands Are Supported

To verify whether a Digi Connect Family device supports a particular command, online help is available. For example:

- **help** displays all supported commands for a device.
- **?** displays all supported commands for a device
- **set** ? displays the syntax and options for the **set** command. Use this command to determine whether the device includes a particular “set” command variant to configure various features.
- **help set** displays syntax and options for the **set** command.
- **set serial ?** displays the syntax and options for the **set serial** command.
- **help set serial** displays the syntax and options for the **set serial** command.

Here are some examples of commands used to configure Digi Connect Family devices. See the Introduction of the *Digi Connect Family Command Reference* for a complete list of features and tasks that can be configured and performed from the command line.

To Configure:	Use This Command:
alarms	set alarms
autoconnection behaviors for serial port connections	set autoconnect
Connectware Device Protocol connection settings	set mgmtconnection
Connectware Device Protocol global settings	set mgmtglobal
Connectware Device Protocol network settings	set mgmtnetwork
Ethernet communications parameters	set ethernet
GPIO pins	set gpio
group attributes: create or establish group attributes, update or remove groups or group attributes	set group
host name	set host
modem emulation	set pmodem
network options	set network
network services	set service
Point-to-Point (PPP) outbound connections	set pppoutbound
port buffering	set buffer
port profile for a serial port	set profiles

To Configure:	Use This Command:
system-identifying information	set system
serial port options--general	set serial
serial TCP and serial UDP	set tcpserial and set udpserial
RealPort configuration options	set realport
RTS toggle	set rtstoggle
SNMP	set snmp
Telnet control command: send Telnet control command to last active Telnet session	send
Telnet operating options	mode
users, user groups, and passwords	set user, set group, newpass
user permissions for various services and command line interface commands	set permissions
wireless devices	set wlan

Configuration through Simple Network Management Protocol (SNMP)

Configuration through Simple Network Management protocol uses a subset of standard MIBs for network and serial configuration, plus several Digi enterprise MIBs for device identification and alarm handling. These MIBs are listed and described on page 58, and must be loaded into a network management station (NMS). The standard and Digi Enterprise MIBs allow for very basic network and serial configuration. For more detailed configuration settings, use the command-line interface or Web user interface instead.

Some elements of SNMP configuration can only be configured from the Web user interface or command line, such as the setting to send alarms as SNMP traps. In the Web user interface, this setting is located at **Configuration > Alarms > *alarm* > Alarm Destinations > Send SNMP trap to following destination when alarm occurs**. See "Configure Alarms" on page 104. In the command-line interface, this setting is configured by the **set alarm** option **type=snmptrap**. See the **set alarm** command description in the *Connect Family Command Reference*.

For more information on SNMP as a device interface, see pages 31 and 57. For information on SNMP as a monitoring interface, see page 154.

Batch Capabilities for Configuring Multiple Devices

For configuring many Digi Connect Family devices at a time, batch configuration capabilities for uploading configuration files are available through the Digi Connect Programmer. For details and command descriptions, see the *Digi Connect Family Customization and Integration Guide.*

What's Next?

See Chapter 3, "Monitoring Capabilities" for details on viewing system information and device statistics and managing device connections and services. Chapter 4, "Administration Tasks" describes common administrative tasks such as file management, updating firmware, and restoring configuration settings to factory defaults.

Monitoring Capabilities

CHAPTER 3

The port, device, system, and network activities of Digi Connect Family products can be monitored for from a variety of interfaces. Changes in data flow may indicate problems or activities that may require immediate attention. In addition, connections and network services can be managed.

This chapter discusses monitoring and connection-management capabilities and tasks in Digi Connect Family products. It covers these topics:

- Monitoring Digi devices from the Web-based and Java applet interface
- Monitoring Digi devices from the command line
- Monitoring capabilities from Connectware Manager
- Monitoring capabilities from SNMP

Monitoring Capabilities in the Web and Java Applet User Interfaces

Several device monitoring and connection-management capabilities are available in the Web user interface and Java applet interface. including system information and statistics, and connection management information.

Display System Information

The System Information pages display information about a Digi device, and are typically used by technical support to troubleshoot problems. To display these pages, go to **Administration > System Information**. System Information pages include general system information, GPIO pin information, including the current state of GPIO pins serial port information, network statistics, and diagnostics.

General System Information

The General page displays the following general system information about the Digi device, which can be useful in device monitoring and troubleshooting.

Information on the General System Information page includes:

Model

The model of the Digi device.

MAC Address

A unique network identifier. All network devices are required to have their own unique MAC address. The MAC address is on a sticker on the Digi device. The number is displayed as 12 hexadecimal digits, usually starting with 00:40:9D.

Firmware Version

The current firmware version running in the Digi device. This information may be used to help locate and download new firmware. Firmware updates can be downloaded from **http://support.digi.com/support/firmware**.

Boot Version

The current boot code version running in the Digi device.

POST Version

The current Power-On Self Test (POST) code version running in the Digi device.

CPU Utilization

The amount of CPU resources being used by the Digi device.

Important: 100% CPU Utilization may indicate encryption key generation is in-progress. A CPU usage this high may indicate that encryption key generation is in-progress. On initial boot, the Digi device generates some encryption key material: an RSA key for SSL/TLS operations, and a DSA key for SSH operations. This key-generation process can take as long as 40 minutes to complete. Until the corresponding key is generated, the Digi device will be unable to initiate or accept that type of encrypted connection. It will also report itself as 100% busy but, since key generation takes place at a low priority, the device will still function normally. On subsequent reboots, the Digi device will use its existing keys and will not need to generate another unless a reset to factory defaults is done, which will cause a new key to be generated on the next reboot.

Up Time

The amount of time the Digi device has been running since it was last powered on or rebooted.

Total/Used/Free Memory

The amount of memory (RAM) available, currently in use, and currently not being used.

GPIO Information

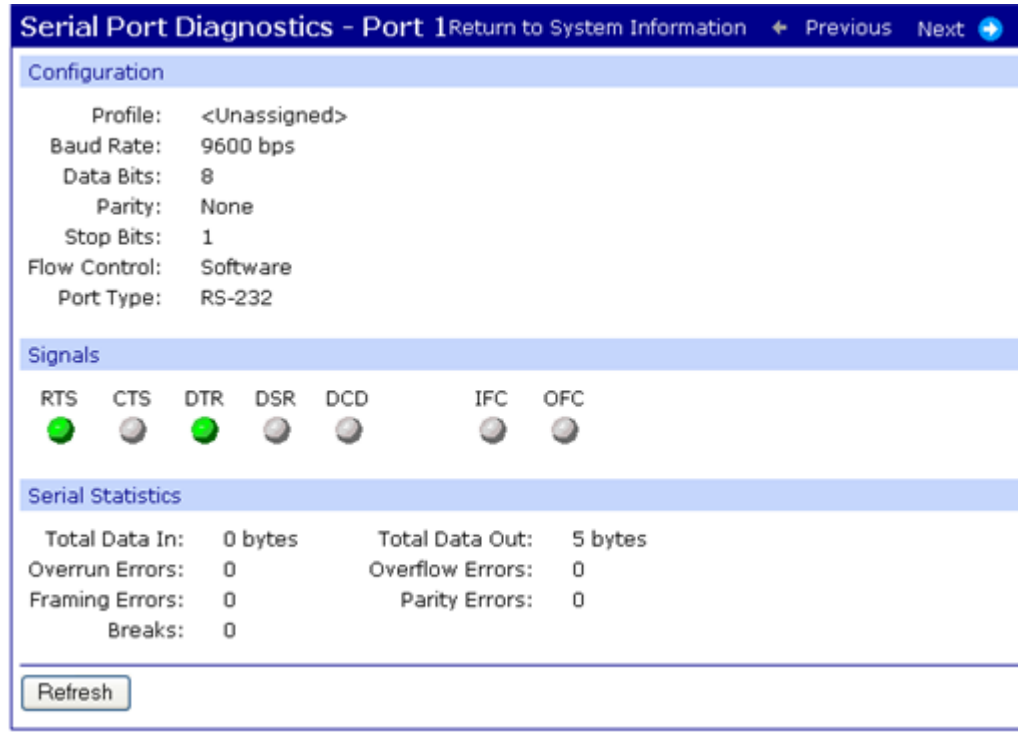
The GPIO page displays the current state of the General Purpose I/O pins on the Digi Connect Family product. The state of pins configured for output can be changed, as discussed in "Configure GPIO Pins" on page 100. Alarms can be issued when GPIO pins change state, as discussed in "Configure Alarms" on page 104.

Serial Port Information

The Serial page of System Information lists the serial ports that are configured for the Digi device. Click on a port to view the detailed serial port information.

Serial Port Diagnostics Page

The Serial Port Diagnostics page of system information provides details that may aid in troubleshooting serial communication problems.



Configuration

The Configuration section of serial port information includes the electrical interface (Port Type) and basic serial settings.

Signals

In the Signals section shows the serial port signals are green when asserted (on) and gray when not asserted (off). The meanings of the signals are:

RTS

Request To Send.

CTS

Clear To Send.

DTR

Data Terminal Ready.

DSR

Data Set Ready.

DCD

Data Carrier Detected.

OFC

Output Flow Control. This signal indicates that flow control is enabled on the remote side of the serial-port connection, and that the Digi device should stop sending data.

IFC

Input Flow Control. This signal indicates that the Digi device is operating as if flow control is enabled for incoming data sent from the remote side of the serial-port connection. This signal is more of an indication that flow control is intended or expected rather than true state information. If the remote side has a flow-control mechanism enabled, the Digi device will use it.

Serial Statistics

The Serial Statistics section of serial port information includes data counters and error tracking that will help determine the quality of data that is being sent or received. If the error counters are accumulating, there may be a problem in the Digi device.

Total Data In

Total number of data bytes received.

Total Data Out

Total number of data bytes transmitted.

Overrun Errors

Number of overrun errors - the next data character arrived before the hardware could move the previous character.

Overflow Errors

Number of overflow errors - the receive buffer was full when additional data was received.

Framing Errors

Number of framing errors received - the received data did not have a valid stop bit.

Parity Errors

Number of parity errors - the received data did not have the correct parity setting.

Breaks

Number of break signals received.

Network Statistics

Network Statistics are detailed statistics about network and protocol activity that may aid in troubleshooting network communication problems. Statistics displayed are those gathered since the unit was last rebooted. If an error counter accumulates at an unexpected rate for that type of counter, there may be a problem in the Digi device.

Ethernet Connection Statistics

Speed

Ethernet link speed: 10 or 100 Mbps. N/A if link integrity is not detected, for example, if the cable is disconnected.

Duplex

Ethernet link mode: half or full duplex. N/A if link integrity is not detected, for example, if the cable is disconnected.

Bytes Received
Bytes Sent

Number of bytes received or sent.

Unicast Packets Received

Number of unicast packets received and delivered to a higher-layer protocol. A unicast packet is one directed to an Ethernet MAC address.

Unicast Packets Sent

Number of unicast packets requested to be sent by a higher-layer protocol. A unicast packet is one directed to an Ethernet MAC address.

Non-Unicast Packets Received

Number of non-unicast packets received and delivered to a higher-layer protocol. A non-unicast packet is one directed to either an Ethernet broadcast address or a multicast address.

Non-Unicast Packets Sent

Number of non-unicast packets requested to be sent by a higher-layer protocol. A non-unicast packet is one directed to either an Ethernet broadcast address or a multicast address.

Unknown Protocol Packets Received

Number of packets received that were discarded because of an unknown or unsupported protocol.

IP Statistics

Datagrams Received
Datagrams Forwarded

Number of datagrams received or forwarded.

Forwarding

Displays whether forwarding is enabled or disabled.

No Routes

Number of outgoing datagrams for which no route to the destination IP could be found.

Routing Discards

Number of outgoing datagrams which have been discarded.

Default Time-To-Live

Number of routers an IP packet can pass through before being discarded.

TCP Statistics

Segments Received
Segments Sent

Number of segments received or sent.

Active Opens

Number of active opens. In an active open, the Digi device is initiating a connection request with a server.

Passive Opens

Number of passive opens. In a passive open, the Digi device is listening for a connection request from a client.

Bad Segments Received

Number of segments received with errors.

Attempt Fails

Number of failed connection attempts.

Segments Retransmitted

Number of segments retransmitted. Segments are retransmitted when the server doesn't respond to a packet sent by the client. This is to handle packets that might get lost or discarded somewhere in the network.

Established Resets

Number of established connections that have been reset.

UDP Statistics

Datagrams Received
Datagrams Sent

Number of datagrams received or sent.

Bad Datagrams Received

Number of bad datagrams that were received. This number does not include the value contained by “No Ports.”

No Ports

Number of received datagrams that were discarded because the specified port was invalid.

ICMP Statistics

Messages Received

Number of messages received.

Bad Messages Received

Number of received messages with errors.

Destination Unreachable Messages Received

Number of destination unreachable messages received. A destination unreachable message is sent to the originator when a datagram fails to reach its intended destination.

Wireless Statistics

The Wireless Statistics section displays more detailed wireless statistics that may aid in troubleshooting network communication problems.

Status

The current status of the wireless device, which may include:

- **Not Connected**: not associated or connected w/ any access point, perhaps because the wireless device has not fully initialized, is out of range, or the wireless interface is disconnected because the Ethernet interface is enabled.
- **Searching for Network**: searching for a wireless network or access point for connection.
- **Associated with Network**: successfully associated with the network w/ the proper network settings and encryption.
- **Authenticated with Network**: successfully authenticated a username/ password with the network when WPA is enabled.
- **Joined Ad Hoc Network**: successfully connected to and joined an ad-hoc network.
- **Started Ad Hoc Network**: successfully created, started, and joined an ad-hoc network.

Network Name

The name of the wireless network to which the device is connected.

Network ID

The ID of the wireless network to which the device is connected and communicating.

Channel

The frequency channel used by the wireless Ethernet radio for the Digi Connect Family device.

Transmit Rate

The current transmission rate for the wireless Ethernet radio.

Signal Strength

The current receive signal strength as reported by the wireless Ethernet radio. Ranges are from 0 to 100.

Diagnostics

The Diagnostics page provides a ping utility to determine whether the Digi device can access remote devices over the network. Enter the hostname of the remote device to attempt to access, and click **Ping**.

Manage Connections and Services

The **Management** menu is for viewing and managing connections and services for the Digi device.

Manage Serial Ports

Management > Serial Ports provides an overview of the serial ports and their connections. Clicking **Connections** displays the active connections for that serial port. The view can be refreshed to see any new serial-port connections list, and connections can be disconnected as needed.

Manage Connections

Management > Connections displays active system connections.

Manage Active System Connections

The **Active System Connections list** provides an overview of connections associated with various interfaces, such as user connections to the device's Web user interface, or to the command line through the local shell; the protocols used for the connections; and the number of active sessions for each connection. One of the uses of this list is to determine whether any connections are no longer needed and can be disconnected.

Monitoring Capabilities from the Command Line

There are several commands for monitoring Digi Connect Family devices and managing their connections. For complete descriptions of these commands, see the *Digi Connect Family Command Reference*.

Commands for Displaying Device Information and Statistics

- **display:** Displays real-time information about a device, such as:
  - General product information, including the product name, MAC address, boot, post, and firmware versions, memory usage, utilization, and uptime, or the amount of time since the device was booted (**display device**).
  - Active interfaces on the system, for example, the Web user interface, command line interface, Point to Point Protocol (PPP), and Ethernet interface, and their status, such as “Closed” or “Connected.” (**display netdevice**).
  - GPIO signals (**display gpio**).
  - Memory usage information (**display memory**).
  - Serial modem signals. (**display serial**).
  - General status of the sockets resource (**display sockets**).
  - Active TCP sessions and active TCP listeners (**display tcp**).
  - Current UDP listeners (**display udp**).
  - Point-to-Point Protocol (PPP) information
  - Uptime information (**display uptime**).

- **info:** Displays statistical information about a device over time. The statistics displayed are those gathered since the tables containing the statistics were last cleared. The **info** command keywords displays the following types of statistics:
  - Device statistics. **info device** displays such details as product, MAC address, boot, POST, and firmware versions, memory usage, utilization, and uptime.
  - Ethernet statistics. **info ethernet** displays statistics regarding the Ethernet interface, including the number of bytes and packets sent and received, the number of incoming and outgoing bytes that were discarded or that contained errors, the number of Rx overruns, the number of times the transmitter has been reset, and the number of incoming bytes when the protocol was unknown.
  - ICMP statistics. **info icmp** displays the number of messages, bad messages, and destination unreachable messages received.
  - Serial statistics. **info serial** displays the number of bytes received and transmitted, signal changes, FIFO and buffer overruns, framing and parity errors, and breaks detected.
  - TCP statistics. **info tcp** displays the number of segments received or sent, the number of active and passive opens, the number of bad segments received, the number of failed connection attempts, the number of segments retransmitted, and the number of established connections that have been reset.
  - UDP statistics. **info udp** displays the number of datagrams received or sent, bad datagrams received, and the number of received datagrams that were discarded because the specified port was invalid.
  - Wireless statistics. **info wlan** displays detailed statistics for wireless devices that may aid in troubleshooting network communication problems with a wireless network.
- **set alarm:** Displays current alarm settings, including the conditions which trigger alarms, and how the alarms are sent, either as an email message, an SNMP trap, or both. The alarms can be reconfigured as needed.
- **set gpio:** Displays current GPIO pin settings. The pin settings can be reconfigured as needed.
- **set buffer and display buffers:** These commands can be used to display port-buffering-related information. **set buffer** configures buffering parameters on a port and displays the current port buffer configuration. **display buffers** displays the contents of a port buffer, or transfers the port-buffer contents to a server running Trivial File Transfer Protocol (TFTP).

- **set snmp:** Configures SNMP, including SNMP traps, such as authentication failure, cold start, link up, and login traps, and displays current SNMP settings.
- **show:** Displays current settings in a device.

Commands for Managing Connections and Sessions

- **close:** Closes active sessions that were opened by **connect**, **rlogin**, and **telnet** commands.
- **connect:** Makes a connection, or establishes a connection, with a serial port.
- **exit** and **quit:** Terminates a currently active session.
- **who and kill: who** displays a global list of connections. The list of connections includes those associated with a serial port or the command-line interface. **who** is particularly useful in conjunction with the **kill** command, which terminates active connections. Use who to determine any connections that are no longer needed, and end the connections by issuing a **kill** command.
- **mode:** Changes or displays the operating options for a current Telnet session.
- **ping:** Tests whether a host or other device is active and reachable.
- **reconnect:** Reestablishes a previously established connection; that is, a connection opened by a **connect**, **rlogin**, or **telnet** command; the default operation is to reconnect to the last active session.
- **rlogin:** Performs a login to a remote system, also referred to as an rlogin.
- **send:** Sends a Telnet control command, such as break, abort output, are you there, escape, or interrupt process, to the last active Telnet session.
- **status:** Displays a list of sessions, or outgoing connections made by **connect**, **rlogin**, or **telnet** commands for a device. Typically, the **status** command is used to determine which of the current sessions to close.
- **telnet:** Makes an outgoing Telnet connection, also known as a session.

Monitoring Capabilities from Connectware Manager

Digi devices can be monitored and managed from Connectware Manager. Examples of activities from Connectware Manager include:

- Displaying detailed state information and statistics about a device, such as device up time, amount of used and free memory, network settings,
- Monitoring the state of the device's connection and see a connection report and connection history statistics.
- Redirecting devices to a to a different destination
- Disconnecting devices
- Removing devices from the network.

See the *Digi Connectware Manager Operator's Guide's* chapters on managing devices and monitoring device statistics and status.

Monitoring Capabilities from SNMP

Device monitoring capabilities from SNMP include, among other things:

- Network statistics, defined in RFC 1213, MIB-II
- Port statistics, defined in RFCs 1316 and 1317
- Device information, defined in Digi enterprise MIB DIGI-DEVICE-INFO.mib

For more information on the statistics available through the standard RFCs listed above, refer to the RFCs available on the IETF web site (**www.ietf.org**). For enterprise MIBs, refer to the description fields in the MIB text.

Administration Tasks

CHAPTER 4

This chapter discusses the administration tasks that need to be performed on Digi Connect Family devices periodically, such as file management, changing the password used for logging onto the device, backing up and restoring device configurations, updating firmware and Boot/POST code, restoring the device configuration to factory defaults, and rebooting the device. As with device configuration and monitoring, it covers performing administrative tasks through a variety of device interfaces.

It covers these main topics:

- Administration from the Web user interface
- Administration from the Java applet interface
- Administration from the command-line interface
- Administration from Connectware Manager

Administration from the Web User Interface

The Administration section of the Web user interface main menu provides the following choices:

- **File Management:** For uploading and managing files, such as custom web pages, applet files, and initialization files. See "File Management" on page 157.
- **Backup/Restore:** For backing up or restoring a device's configuration settings. See "Backup/Restore Device Configurations" on page 158.
- **Update Firmware:** For updating firmware, including Boot and POST code. See "Update Firmware and Boot/POST Code" on page 159.
- **Factory Default Settings:** For restoring a device to factory default settings. See "Restore a Device Configuration to Factory Defaults" on page 160.
- **System Information:** For displaying general system information for the device and device statistics. See "Display System Information" on page 163.
- **Reboot:** For rebooting the device. See "Reboot the Digi Device" on page 163.

These administrative tasks are organized elsewhere in the Web user interface:

- Enable and disable network services. See "Network Services Settings" on page 84.
- Enable password authentication for the Digi Connect Family device. See "Configure User Settings" on page 114.

File Management

The **File Management** page of the Web user interface uploads custom files to a Digi Connect Family device, Custom applets allow the flexibility to alter the interface either by adding a different company logo, changing colors, or moving information to different locations. If custom applets or the sample Java applet is not used, using this feature is not necessary.Uploading Files

To upload files to a Digi Connect Family device, enter the file path and name for the file, or click **Browse** to locate and select the file, and click **Upload**.

Delete Files

To delete files from a Digi Connect Family device, select the file from the list under **Manage Files** and click **Delete**.

Custom Files Are Not Deleted By Device Reset

Any files uploaded to the file system of a Digi Connect Family device from the File Management page are not deleted by restoring the device configuration to factory defaults, or by pressing the Reset button on the device (see "Restore a Device Configuration to Factory Defaults" on page 160). This deletion is prevented so that customers with custom applets and custom factory defaults can retain them on the device and not have them deleted by a reset. Such files can only be deleted by the Delete operation, described above.

Backup/Restore Device Configurations

Once a Digi Connect Family device is configured, backing up the configuration settings is recommended in case problems occur later, firmware is upgraded, or hardware is added. If multiple devices need to be configured, the backup/restore feature can be used as a convenience, where the first device's configuration settings is backed u to a file, then the file is loaded onto the other devices.

This procedure shows how to back up or restore the configuration to a server and download a configuration from a server to a file or TFTP.

If using TFTP, ensure that the TFTP program is running on a server.

1. From the Main menu, click **Administration > Backup/Restore**. The Backup/Restore page is displayed.

2. Choose the appropriate option (**Backup** or **Restore**) and select the file.

Update Firmware and Boot/POST Code

The Digi Connect Family device's firmware and/or boot/POST code can be updated from a file on a PC or through TFTP.The recommended method is to download the firmware to a local hard drive. TFTP is supported for those using UNIX systems. Both the firmware and the boot/POST code are updated using the same set of steps. The Digi Connect Family device automatically determines the type of image being uploaded. Before uploading the firmware or the boot/POST code, it is very important to read the Release Notes supplied with the firmware to check if the boot/POST code must be updated before updating the firmware.

Prerequisites

These procedures assume that:

- A firmware file has already been downloaded the firmware file from the Digi web site.
- If using TFTP, that TFTP is running.

Update Firmware from a File on a PC

1. From the Main menu, click **Administration > Update Firmware**. The Update Firmware page is displayed.
2. Enter the name of the firmware or POST file in the **Select Firmware** edit box, or click **Browse** to locate and select the firmware or POST file.
3. Click **Update**.

   Important: DO NOT close the browser until the update is complete and a reboot prompt has been displayed.

Update Firmware from a TFTP Server

Updating firmware from a TFTP server is done from the command-line interface using the **boot** command. It cannot be done from the Web user interface. For details, see "Administration from the Command-Line Interface" on page 167.

Restore a Device Configuration to Factory Defaults

Restoring a Digi Connect Family device to its factory default settings clears all current configuration settings except the IP address settings and host key settings. In addition, any files that were loaded into the device through the File Management page such as custom-interface files and applet files are retained. See "File Management" on page 157 for information on loading and deleting files.

There are two ways to reset the device configuration of a Digi Connect Family device to the factory default settings: from the Web user interface and using the reset button on the Digi device.

What Is Cleared and Retained During a Factory Reset

The **Restore Factory Defaults** operation clears all current settings *except* the IP address settings and host key settings. This is the best way to reset the configuration, because the settings can also be backed up using the Backup/Restore operation, which provides a means for restoring it after the configuration issues have been resolved.

Using the Web User Interface

1. Make a backup copy of the configuration using the Backup/Restore operation, described on page 158.
2. From the Main menu, click **Administration > Factory Default Settings**. The Factory Default Settings page is displayed.
3. Choose whether to keep the network settings for the device, such as the IP address, and click **Restore.**

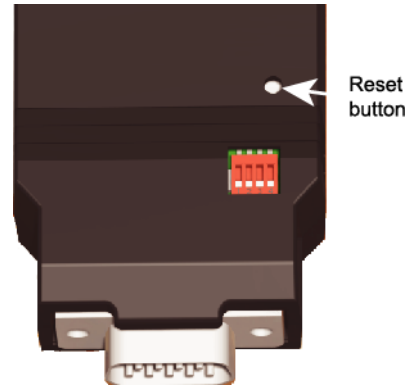
Using the Reset Button

If the Digi device cannot be accessed from the Web user interface, the configuration can be restored to factory defaults by using the Reset button.

Reset Digi Connect SP and Digi Connect Wi-SP

1 Power off the Digi Connect device by unplugging the power.

2 Locate the Reset button on the device, as shown in the figure. Use a non-conducive, small diameter tool (such as wood or plastic) with a blunt end (NOT SHARP or the button could be damaged) to press gently and hold down the reset button. The flashing sequence of LEDs may take several seconds.



3 While holding the Reset button, power up the unit.

4 Hold the button for 20 seconds and then release it.

The default configuration is restored. When the restoration is complete, the device flashes a code (1-5-1).

Reset Digi Connect ME and Digi Connect Wi-ME

To restore the configuration on a Digi Connect ME or Digi Connect Wi-ME to factory defaults, short pin 20 (the /init pin) to ground during boot up to factory default the module. Note that shorting pin 14 simply reboots the unit but does not restore the configuration.

Reset Digi Connect EM or Digi Connect Wi-EM

1. Power off the Digi Connect device.
2. Locate the Reset switch between P3 and CR1

3. Power on the device while holding the Reset switch down. (Hold it down for about 20 seconds.)
4. When the device is prepared to reset, it flashes a code (1-5-1) on the red LED.
5. Release the switch to reset the configuration to factory defaults.

Display System Information

System information displays the model, MAC address, firmware version, boot version, and POST version of the Digi Connect Family device. It also displays memory available: total, used, and free, and tracks CPU percent utilization and the uptime.

From the main menu, click **Administration > System Information**. Select **General**, **GPIO**, **Serial** or **Network** for the appropriate information. For descriptions of the information displayed on these screens, see page 140.

Reboot the Digi Device

Changes to some device settings require saving the changes and rebooting the Digi Connect Family device. To reboot a Digi device:

1. From the main menu, click **Administration > Reboot**.
2. On the **Reboot** page, click the **Reboot** button. Wait approximately 1 minute for the reboot to complete.

Enable/Disable Access to Services

As needed, enable and disable access to various network services, such as ADDP, RealPort, SNMP, and Telnet. For example, for performance and security reasons, it may be desirable to disable access to all network services not necessary for running or interfacing with the Digi Connect Family device. In the Web user interface, enabling and disabling network services is done on the Network Configuration page for a device. See "Network Services Settings" on page 84.

Administration from the Java Applet Interface

In the Java applet device interface, administration tasks are also organized under **Administration** in the main menu. There are fewer choices than in the Web user interface:

- **Backup/Restore:** Backs up or restores a Digi device configuration.
- **Restore Factory Defaults:** Restores a Digi device's configuration to factory defaults.
- **System Information:** Displays system information for the device, including general device information, current GPIO pin settings, serial line signals and statistics, and network statistics.
- **Reboot:** Reboots the Digi device.

File management tasks or firmware updates cannot be performed from the Java applet interface. To perform such tasks, switch the device interface to the Web user interface.

Additionally, over time, network services may need to be disabled or enabled. See "Network Services Settings" on page 84.

Backup/Restore Device Configurations

1. If using TFTP, ensure that the TFTP program is running on a server.
2. From the main menu, click **Administration > Backup/Restore** from the main menu.
3. Choose the appropriate option (**Backup** or **Restore**) and select the file.

Restore Device Configuration to Factory Defaults

There are two ways to restore the device configuration to the factory default settings:

- Reset the configuration from a web browser, which clears all current device configuration settings except the IP address settings and administrator password. This is the best way to reset the configuration as it allows for backing up the settings, providing a means for restoring the settings after any configuration issues are resolved. See "Using the Web User Interface" on page 160 for more information.
- Reset the configuration using the reset button on the Digi Connect device. Use this method if the device cannot be accessed from a web browser. The location of the reset button may vary. See "Using the Reset Button" on page 161.

What Is Cleared and Retained During a Factory Reset

Restoring the Digi Connect device to its factory default settings clears all current settings *except* the IP address settings and the administrator password. Any files such as custom-interface files and applet files that were loaded through the Web user interface's **File Management** page are retained. See "File Management" on page 157 for information on loading and deleting files.

Restore the Configuration from a Browser

1. From the main menu, click **Administration > Factory Default Settings**.
2. Click **Restore.**

Display System Information

System information displays the model, MAC address, and the version levels for firmware, boot code, and POST code in the Digi Connect device. It also displays memory available–total, used, and free, and tracks CPU percent utilization and the uptime.To display system information, from the main menu, click **Administration > System Administration**. Select **General**, **GPIO**, **Serial** or **Network** for the appropriate information.

Reboot the Device

Some changes to configuration settings require saving the changes and rebooting the Digi device. To reboot, from the main menu, click **Administration > Reboot.** Click the **Reboot** button, and wait approximately 1 minute for the reboot to complete.

Enable/Disable Access to Services

As needed, enable and disable access to various network services, such as ADDP, RealPort, SNMP, and Telnet. For example, for security or performance reasons, it may be desired to disable services that are not necessary for running or interfacing with the Digi Connect device. In the Java applet interface, enabling and disabling network services is done on the **Network Services** tab of the **Network Configuration** page. See "Configure Network Communications" on page 78.

Administration from the Command-Line Interface

Administrative tasks can also be performed from the command line. Here are several device-administration tasks and the commands used to perform them. See the *Digi Connect Family Command Reference* for more complete command descriptions.

Administrative Task	Command
Backup/restore a configuration from a TFTP server on the network	backup
Update firmware	boot ■ Telnet to the Digi device's command line interface using a telnet application or hyperterm. ■ If security is enabled for the Digi device, a login prompt is displayed. The default username is “root” and the default password is “dbps.” If these defaults do not work, contact the system administrator who set up the device. ■ Issue the command: #> boot load=*tftp-server-ip*:*filename* where *tftp-server-ip* is the IP address of the TFTP server that contains the firmware, and *filename* is the name of the file to upload.
Reset configuration to factory defaults	revert or boot action=factory
Display system information and statistics	info
Reboot the device	boot
Enable/disable network services	set service

Specifications and Certifications

CHAPTER 5

This chapter provides hardware specifications, additional feature detail, and regulatory statements and certifications for Digi Connect Family products.

- Hardware specifications
- Regulatory statements and certifications

Hardware Specifications

See Hardware References for most Connect Family Product Specifications

Several Digi Connect products have *Hardware Reference Manuals*, which include hardware specifications. The specifications listed here are for products that do not have an accompanying *Hardware Reference Manual*.

Digi Connect ES Specifications

Specification		Value
Environmental	Ambient temperature	0^{o} - 55^{o}C (32^{o} to 130^{o} F)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	30^{o} to 85^{o} C (-122^{o} to 185^{o} F)
	Altitude	3657.6 meters (12000 feet)
	Serial Port Protection (ESD)	Serial Port Protection (ESD): +15 kV human body model
Power requirements	External	100-240V
	Input frequency	50-60 Hz
	Input current protection	1.0 A / 250 V(Time Lag) rated fuse
	UL certified	Yes
	Surge protection	■ 4 kV burst (EFT) per EN61000-4-4 ■ 4 kV isolation input to output ■ 2 kV surge per EN61000-4-5
Mechanical dimensions	Length	23.5 cm (9.3 in)
	Width	26.9 cm (10.6 in)
	Depth	4.2 cm (2.1 in)

ConnectPort TS 8 Specifications

Specification		Value
Environmental	Ambient temperature	0° - 60°C (32° to 140° F)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	-40° to 85° C (-40° to 185° F)
	Altitude	3657.6 meters (12000 feet)
	Serial Port Protection (ESD)	Serial Port Protection (ESD): +15 kV human body model
Power requirements	DC power range	9-30V
	Typical Power Consumption DC Current @ 120 Vdc (mA)	6W (500mA @ 12Vdc)
	Max Power Consumption (watts)	12W (1A @ 12Vdc)
	Recommended Power Supply Input Rating (watts)	17W (120Vac * .14A) External power supply provided with product purchase
	UL certified	Yes
Mechanical dimensions	Length	10.5 cm (4.15 in)
	Width	19.6 cm (7.7 in)
	Depth	3.3 cm (1.3 in)
USB interface	Input	500mA max

Wireless Networking Features

Here are key wireless-networking features that can be configured in Digi Connect wireless products (Digi Connect Wi-ME, Digi Connect Wi-EM, and Digi Connect Wi-SP). For more details and up-to-date information on support of these features, see the readme file for your Digi Connect product.

Feature	Description
Wireless Modulation	CCK (11/5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
Wireless Transmit Power	16 dBm
Wireless Receive Sensitivity	-82 dBm at 11 Mbps
Wireless Antenna Connector	1 x RP-SMA for Digi Connect Wi-ME, Wi-SP. 2 x RP-SMA for Digi Connect Wi-EM.
Country Code	Specifies the country in which the product is used.
Network Mode	■ Open ■ Infrastructure Mode ■ Ad-Hoc Mode
Channel	Can use automatic channel search-and-select or a user-configurable channel number.
Data Rate	Auto, 1Mbps, 2Mbps, 5.5Mbps, 11Mbps
Service Set Identifier (SSID)	A user-configurable SSID string or auto-connect option.
Wireless Security	Wi-Fi Protected Access (WPA/WPA2/802.11i) Wired Equivalent Privacy (WEP)
Authentication Options	■ Open ■ Shared ■ Wi-Fi Protected Access (WPA2/802.11i) ■ WPA/WPA2 with pre-shared key (WPA-PSK)
802.1x (WPA2/802.11i) Authentication	Protected Extensible Authentication Protocol (PEAP) with EAP- MS
Encryption	■ Temporal Key Integrity Protocol (TKIP) ■ Counter mode CBC MAC Protocol (CCMP) ■ Wired Equivalent Privacy (WEP) ■ Use of encryption can be disabled.

Feature	Description
Network Key	A shared key (ASCII or Hexadecimal) to be used for WEP or WPA-PSK.
Username	A username to be specified when 802.1x -based authentication (WPA) is used.
Password	A password to be specified when 802.1x based authentication (WPA) is used.
EkahauClient™	Provides integrated support for Ekahau's Wi-Fi device-location solution. Ekahau offers a complete access point vendor-independent real-time location system for wireless LAN devices that is capable of pinpointing wireless LAN devices such as the Digi Connect products, laptops, PDAs, or other intelligent Wi-Fi enabled devices. The solution provides floor-, room- and door-level accuracy of up to 3.5 feet (1 m). The patented Ekahau positioning technology is based on simple signal-strength calibration maps, and enables customers to fully leverage an existing wireless LAN infrastructure without any need for proprietary hardware components.
Wireless Networking Status Features:	The following status information can be displayed for Wireless Digi Connect devices. For more detailed descriptions, see "Wireless Statistics" on page 148.
Connection Status	The status of the wireless network connection.
Network Mode	The network mode currently in use: ■ Infrastructure Mode ■ Ad-Hoc Mode
Access Points	Information related to the associated access point, such as MAC address, and a list of all detected wireless networks.
Data Transfer Rate	The data transfer rate of the current connection.
Channel	The wireless network channel currently in use.
SSID	The selected SSID of the wireless network.
Wireless Security: Wi-Fi Protected Access (WPA/WPA2/802.11i), Wired Equivalent Privacy (WEP) security and encryption	The status of the WEP/WPA/WPA2 security features, including the Authentication Method currently in use and whether authentication is enabled or disabled
Signal Strength	A statistic that indicates the strength of the radio signal between 0 and 100 percent.

Regulatory Information and Certifications

RF Exposure Statement

Digi Connect Wi-SP, Digi Connect Wi-EM, and Digi Connect Wi-ME

The Digi Connect Wi-EM and Wi-ME embedded modules comply with the RF exposure limits for humans as called out in RSS-102.

These devices are exempt from RF evaluation based on its operating frequency of 2400 MHz, and effective radiated power of 100 milliwatts. This would be less than the 3 watt requirement for a mobile device (>20 cm separation) operating at 2400 MHz.

FCC Certifications

The FCC certifications in this section are for Digi Connect ES and ConnectPort TS8. For certifications for other Digi Connect devices, see the device's *Hardware Reference*.

FCC Part 15 Class A

These devices comply with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) These devices may not cause harmful interference, and (2) These devices must accept any interference received, including interference that may cause harmful operation.

Radio Frequency Interference (RFI) (FCC 15.105)

This equipment has been tested and found to comply with the limits for Class A digital devices pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, 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 and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the 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.

Labeling Requirements (FCC 15.19)

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications (FCC 15.21)

Changes or modifications to this equipment not expressly approved by Digi may void the user's authority to operate this equipment.

Cables (FCC 15.27)

Shielded cables *must* be used to remain within the Class A limitations.

Industry Canada

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

International EMC (Electromagnetic Emissions/Immunity) Standards

For Digi Connect ES

- EN60601-1-2:2001
- EN55011:1998
- EN55022:1998
- EN55024:1998
- AS/NZS CISPR 22: 2002
- ICES-003, Issue 3:1997
- FCC P15 Subpart B Class A

For ConnectPort TS 8 and ConnectPort TS 8 MEI

- EN55022
- AS/NZS CISPR 22: 2004
- ICES-003, Issue 3:1997
- FCC P15 Subpart B Class A
- EN55024

Safety Standards

There are no user serviceable parts inside the Digi Connect Family products. Contact your Digi representative through "Digi Contact Information" on page 15 for repair information.

For Digi Connect ES

- IE60950-1
- UL60950-1
- CAN/CSA C22.2 No. 60950-1-3
- IEC60601-1

For ConnectPort TS 8 and ConnectPort TS 8 MEI

- IEC60950-1
- UL60950-1
- CAN/CSA C22.2 No 60950-1-3

Important Safety Information

To avoid contact with electrical current:

- Never install electrical wiring during an electrical storm.
- Never install an Ethernet connection in wet locations unless that connector is specifically designed for wet locations.
- Use caution when installing or modifying Ethernet lines.
- Use a screwdriver and other tools with insulated handles.
- Wear safety glasses or goggles.
- Do not place Ethernet wiring or connections in any conduit, outlet or junction box containing electrical wiring.
- Installation of inside wire may bring you close to electrical wire, conduit, terminals and other electrical facilities. Extreme caution must be used to avoid electrical shock from such facilities. Avoid contact with all such facilities.
- Ethernet wiring must be at least 6 feet from bare power wiring or lightning rods and associated wires, and at least 6 inches from other wire (antenna wires, doorbell wires, wires from transformers to neon signs), steam or hot water pipes, and heating ducts.
- Do not place an Ethernet connection where it would allow a person to use an Ethernet device while in a bathtub, shower, swimming pool, or similar hazardous location.
- Protectors and grounding wire placed by the service provider must not be connected to, removed, or modified by the customer.
- Do not touch uninsulated Ethernet wiring if lightning is likely!
- External Wiring: Any *external* communications wiring installed needs to be constructed to all relevant electrical codes. In the United States this is the National Electrical Code Article 800. Contact a licensed electrician for details.

Glossary

802.11

The IEEE standard for wireless Local Area Networks. It uses three different physical layers, 802.11a, 802.11b and 802.11g.

access control list

See IP filtering.

ADDP

See Advanced Device Discovery Protocol.

Address Resolution Protocol (ARP)

A protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

Advanced Digi Discovery Protocol (ADDP)

A protocol that runs on any operating system capable of sending multicast IP packets on a network. ADDP allows the system to identify all ADDP-enabled Digi devices attached to a network by sending out a multicast packet. The Digi devices respond to the multicast packet and identify themselves to the client sending the multicast.

alarms

In Digi Connect devices, alarms are used to send emails or issue SNMP traps when certain device events occur. These events include changes in GPIO signals, certain data patterns being detected in the data stream.

ARP

See Address Resolution Protocol.

autoconnection

A network connection initiated from a Digi device that is based on timing, serial activity, or serial modem signals.

Auto-IP

A standard protocol that automatically assigns an IP address from a reserved pool of standard Auto-IP addresses to the computer on which it is installed. The device is set to obtain its IP address automatically from a Dynamic Host Configuration Protocol (DHCP) server. But if the DHCP server is unavailable or nonexistent, Auto-IP will

assign the device an IP. If DHCP is enabled or responds later or you use ADDP, both will override the Auto-IP address previously assigned. Also referred to as Auto-IP.

CLI

Command-line interface.

COM port redirection

The process of establishing a connection between the host and networked serial devices by creating a local COM or TTY port on the host. See also RealPort.

configuration applet

See Java applet interface.

configuration management

For Digi Connect devices, configuration management involves managing the files and settings that contain device configuration information. Configuration management tasks include copying device configuration files to and from a remote host, upgrading device firmware, and resetting the device configuration to factory defaults.

CTS

Clear to Send.

device server

A one- or two-port intelligent network device that converts serial data into network data.

DHCP

See Dynamic Host Configuration Protocol.

Digi Device Setup Wizard

A wizard for configuring Connect devices that is provided on the CD shipped with each device. The Digi Device Setup Wizard is available in Microsoft Windows or UNIX platforms. It assigns an IP address for the device, configures the device based on your description of the device environment, and determines whether you need to install RealPort. Using the Digi Device Setup Wizard is the recommended and preferred method for configuration.

DSR

Data Set Ready.

DTR

Data Terminal Ready.

Dynamic Host Configuration Protocol (DHCP)

An Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information.

EIA

See Electronics Industry Association.

Electronics Industry Association (EIA) and Electronics Industries Alliance (EIA)

1) The Electronic Industries Association (EIA) comprises individual organizations that together have agreed on certain data transmission standards such as EIA/TIA-232 (formerly known as RS-232).

2) The Electronics Industries Alliance (EIA) is an alliance of trade organizations that lobby in the interest of companies engaged in the manufacture of electronics-related products.

encryption

The conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts.

factory defaults

The default configuration values that are set in a device at the factory.

File Transfer Protocol (FTP)

A standard Internet protocol that specifies the simplest way to exchange files between computers on the Internet.

FTP

See File Transfer Protocol.

General Purpose I/O (GPIO)

On Digi Connect devices, pins that are used for serial communications. In normal operation, the GPIO pins are used for the serial CTS, DCD, DSR, DTR, and RTS. For Digi Connect EM and Wi-EM devices, there are GPIO pins for the TXD and RXD signals. GPIO pins can be configured for different purposes, and alarms can be configured to alert users of a change in GPIO pin state.

GPIO

See General Purpose I/O.

HTTP

See HyperText Transfer Protocol.

HTTPS

See HyperText Transfer Protocol over Secure Socket Layer.

HyperText Transfer Protocol (HTTP)

An application protocol in the TCP/IP suite that defines the rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web (WWW).

HyperText Transfer Protocol over Secure Socket Layer (HTTPS)

A secure message-oriented communications protocol designed for use in conjunction with HTTP. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses the Secure Socket Layer (SSL) as a sublayer.

ICMP

See Internet Control Message Protocol.

IGMP

See Internet Group Management Protocol.

Internet Control Message Protocol (ICMP)

A message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and "broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.

IP filtering

A network configuration that can be enabled to establish rules allowing devices to permit or deny specific IP addresses, networks, or devices from connection access. Also known as access control list.

Java applet interface

An optional Java-applet based Web interface for configuring, monitoring, and administering Digi Connect products.

MAC address

A unique network identifier. All network devices are required to have their own unique MAC address. The MAC address is on a sticker on your Digi device server. The number is displayed as 12 hexadecimal digits, usually starting with 00:40:9D.

Management Information Base (MIB)

A formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP).

MIB

See Management Information Base.

modem emulation

A serial port configuration where the port acts as a modem. The Digi device emulates modem responses to a serial device and seamlessly sends and receives data over an Ethernet network instead of a Public Switched Telephone Network (PSTN). The advantage for a user is the ability to retain legacy software applications without modification and use a less expensive Ethernet network in place of public telephone lines. Also known as pseudo-modem or pmodem.

NAT

NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network through a NAT table that does the global-to-local and local-to-global IP address mapping. This increases security since each outgoing or incoming request must go through a translation process that also authenticates the request or matches it to a previous request. NAT can be statically defined or it can be set up to dynamically translate from and to a pool of IP addresses. NAT also conserves on the number of global IP addresses needed and it uses a single IP address in its communication with the world.

PEAP

See Protected Extensible Authentication Protocol.

port forwarding

A serial port configuration that sends data directly to a specific port instead of the path determined by the router based on traffic.

POST

See Power-On Self Test.

Power-On Self Test (POST)

When power is turned on, POST (Power-On Self-Test) is the diagnostic testing sequence that a computer's basic input/output system (or “starting program”) runs to determine if the computer keyboard, random access memory, disk drives, and other hardware are working correctly.

If the necessary hardware is detected and found to be operating properly, the computer begins to boot. If the hardware is not detected or is found not to be operating properly, the BIOS issues an error message which may be text on the display screen and/or a series of coded beeps, depending on the nature of the problem.

Protected Extensible Authentication Protocol (PEAP)

A protocol proposed for securely transporting authentication data, including passwords, over 802.11 wireless networks. PEAP makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs.

RCI

See Remote Command Interface.

RealPort

RealPort is patented Digi software for COM port redirection. RealPort makes it possible to establish a connection between the host and networked serial devices by creating a local COM or TTY port on the host. The COM/TTY port appears and behaves as a local port to the PC or server. This process of COM port redirection allows existing software applications like DNP3 and Modbus to work without modification. Unlike other COM port redirectors, RealPort offers full hardware and software flow control, as well as tunable latency and throughput. These features ensure optimum performance, since data transfer is adjusted according to specific application requirements.

Remote Command Interface (RCI)

A programmatic interface for configuring and controlling Connect family devices. RCI is an XML-based request/response protocol that allows a caller to query and modify device configurations, access statistics, reboot the device, and reset the device to factory defaults.

Unlike other configuration interfaces that are designed for a user, such as the command-line or browser interfaces, RCI is designed to be used by a program. A typical use of RCI is in a Java applet that can be stored on the Connect device to replace the browse interface with a custom browser interface. Another example is a custom application running on a PC that monitors and controls an installation of many Connect devices.

remote login (rlogin)

A remote login to a Digi Connect device's command-line interface (CLI). rlogin is a Unix command that allows an authorized user to login to other UNIX machines (hosts) on a network and to interact as if the user were physically at the host computer. Once logged in to the host, the user can do anything that the host has given permission for, such as read, edit, or delete files.

remote shell (rsh)

A Berkeley Unix networking command to execute a given command on a remote host, passing it input and receiving its output. Rsh communicates with a daemon on the remote host.

rlogin

See remote login.

RSH

See remote shell.

RTS

Ready to Send.

RXD

Receiving Data.

Secure Sockets Layer (SSL)

A commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.

serial bridge

A connection between two serial devices over a network that acts as if they were connected over a serial cable. Also known as serial tunneling.

serial tunneling

See serial bridge.

Setup Wizard

See Digi Device Setup Wizard.

Simple Mail Transfer Protocol (SMTP)

A TCP/IP protocol used in sending and receiving e-mail. Since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. SMTP usually is implemented to operate over Internet port 25. An alternative to SMTP that is widely used in Europe is X.400. Many mail servers now support Extended Simple Mail Transfer Protocol (ESMTP), which allows multimedia files to be delivered as e-mail.

Simple Network Management Protocol (SNMP)

A protocol for managing and monitoring network devices. The SNMP architecture enables a network administrator to manage nodes--servers, workstations, routers, switches, hubs, etc.--on an IP network; manage network performance, find and solve network problems, and plan for network growth. Digi devices support SNMP Version 1.

SNMP

See Simple Network Management Protocol.

SMTP

See Simple Mail Transfer Protocol.

SSL

See Secure Sockets Layer.

static IP address assignment

The process of assigning a specific IP address to a device. Contrast with assigning a device through Dynamic Host Configuration Protocol (DHCP), or Automatic Private IP Addressing (APIPA or Auto-IP).

TCP

See Transmission Control Protocol.

Telnet

A user command and an underlying TCP/IP protocol for accessing remote computers. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

Temporal Key Integrity Protocol (TKIP)

Part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of the Wired Equivalent Privacy (WEP), which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, and addresses several design shortcomings of the original WEP.

TFTP

See Trivial File Transfer Protocol (TFTP).

TLS

See Transport Layer Security.

Transmission Control Protocol (TCP)

A set of rules used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP handles the actual delivery of the data, TCP handles keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to you from a Web server, the TCP program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end (the client program in your computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

Transport Layer Security (TLS)

A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

Trivial File Transfer Protocol (TFTP)

An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in Request for Comments (RFC) 1350.

TTY port redirection

The process of establishing a connection between the host and networked serial devices by creating a local TTY port on the host. The TTY port appears and behaves as a local port to the PC or server.

See also RealPort.

TXD

Transmit eXchange Data.

UDP

See User Datagram Protocol.

User Datagram Protocol (UDP)

A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP does not provide sequencing of the packets in which the data arrives, nor does it guarantee delivery of data. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

In the Open Systems Interconnection (OSI) communication model, UDP, like TCP, is in layer 4, the Transport Layer.

Web user interface

The Web-based interface for configuring, monitoring, and administering Digi Connect devices that is provided for Digi Connect devices by default.

WEP

See Wired Equivalent Privacy.

Wired Equivalent Privacy (WEP)

A data encryption method used to protect the transmission between 802.11 wireless clients and APs. See also Temporal Key Integrity Protocol (TKIP).

Wi-Fi Protected Access (WPA)

A data encryption/ user authentication method for 802.11 wireless LANs. WPA uses the Temporal Key Integrity Protocol (TKIP).

WPA

See Wi-Fi Protected Access.

WPA2/802.11i

WPA with AES-based encryption (CCMP)

Index

D

E

O

P

T


Digi®