Ref. Certif. No.

US/12867/UL

IEC SYSTEM FOR CONFORMITY TESTING AND CERTIFICATION OF ELECTRICAL EQUIPMENT (IECEE) CB SCHEME

SYSTEME CEI D'ESSAIS DE CONFORMITE ET DE CERTIFICATION DES EQUIPEMENTS ELECTRIQUES (IECEE) METHODE OC

CB TEST CERTIFICATE
CERTIFICAT D'ESSAI OC

Product
Produit

Ethernet to Serial Converter

Name and address of the applicant
Nom et adresse du demandeur

Digi International Inc
11001 Bren Rd E
Minnetonka, MN 55343, USA

Name and address of the manufacturer
Nom et adresse du fabricant

Digi International Inc
11001 Bren Rd E
Minnetonka, MN 55343, USA

Name and address of the factory
Nom et adresse de l'usine

Digi International Inc.
10000 W 76 St
Eden Prairie, MN 55344, USA

Rating and principal characteristics
Valeurs nominales et caractéristiques principales

100-240 V ac, 50-60 Hz 0.24 A maximum

Trademark (if any)
Marque de fabrique (si elle existe)

Model / Type Ref.
Ref. de type

50001544-xx where x may be any alphanumeric character indicating changes in SELV circuitry.

Additional information (if necessary)
Information complémentaire (si nécessaire)

This CB Test Report comprises 6 enclosures.

A sample of the product was tested and found to be in conformity with
Un échantillon de ce produit a été essayé et a été considéré conforme à la

PUBLICATION	EDITION
IEC 60950-1 (2001)	**First Edition,**

Additional evaluation to CENELEC Common Modifications also included.
See Test Report for National Differences.

as shown in the Test Report Ref. No.
which forms part of this Certificate
comme indiqué dans le Rapport d'essais numéro de référence qui constitue partie de ce Certificat

E165880-A46-CB-1

This CB Test Certificate is issued by the National Certification Body
Ce Certificat d'essai OC est établi par l'Organisme National de Certification

Underwriters Laboratories

Underwriters Laboratories Inc. / Certification Programs Office, USA
333 Pfingsten Road, Northbrook, IL 60062-2096
United States of America
TEL INT* +1 847 664 3008, FAX INT* +1 847 313 3008
email: jolanta.m.wroblewska@us.ul.com

Date:
Issued: 2008 July 21

Signature:

Jolanta M. Wroblewska

COVER PAGE FOR TEST REPORT

Test Item Description:	Ethernet to Serial Converter
Model/Type Reference:	50001544-xx where x may be any alphanumeric character indicating changes in SELV circuitry.
Rating(s):	100-240 V AC, 50-60 Hz 0.24 A maximum
Standards:	IEC 60950-1:2001, First Edition
Applicant Name and Address:	DIGI INTERNATIONAL INC 11001 BREN RD E MINNETONKA MN 55343 UNITED STATES
Factory Location(s):	DIGI INTERNATIONAL INC. 10000 W 76 ST EDEN PRAIRIE, MN 55344 USA

This Report includes the following parts, in addition to this cover page:

1. Specific Technical Criteria
2. Clause Verdicts
3. Critical Components
4. Test Results
5. Enclosures
    a. National Differences
    b. Marking Plate
    c. Photographs
    d. Manuals
    e. Miscellaneous
    f. Licenses

All applicable tests according to the above standard(s) have been carried out.
Test results are valid only for the tested equipment.
This Test Report can be reproduced only in whole.
Amendments and corrections can be reproduced only with the original CB Test Report.
Written permission from Underwriters Laboratories Inc. is required if the test report is copied in part.

Test Report issued under the responsibility of:

Underwriters Laboratories Inc.

TEST REPORT
IEC 60950-1,First Edition
Information technology equipment-Safety
Part 1:General Requirements

Report Reference No ..... :	E165880-A46-CB-1
Date of issue ..... :	2008-07-21
Total number of pages ..... :	42
CB Testing Laboratory ..... :	Underwriters Laboratories Inc.
Address ..... :	333 Pfingsten Road, Northbrook, IL, 60062-2096, USA
Applicant's name ..... :	DIGI INTERNATIONAL INC
Address ..... :	11001 BREN RD E MINNETONKA MN 55343 UNITED STATES
Test specification:	
Standard ..... :	IEC 60950-1:2001, First Edition
Test procedure ..... :	CB Scheme
Non-standard test method ..... :	N/A
Test Report Form No. ..... :	IEC60950_1B
Test Report Form originator ..... :	SGS Fimko Ltd
Master TRF ..... :	dated 2003-03

This report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

Test item description ..... :	Ethernet to Serial Converter
Trade Mark ..... :	
Model/Type reference ..... :	50001544-xx where x may be any alphanumeric character indicating changes in SELV circuitry.
Manufacturer ..... :	DIGI INTERNATIONAL INC. 11001 BREN ROAD EAST MINNETONKA, MN 55343, USA
Rating ..... :	100-240 V AC, 50-60 Hz 0.24 A maximum

Testing procedure and testing location:			
[ ]	**CB Testing Laboratory**		
	Testing location / address..... :		
[x]	**Associated CB Test Laboratory**		
	Testing location / address..... :	Underwriters Laboratories Inc. 3550 Labore Road, Suite 1, Vadnais Heights, MN, 55110, USA	
	Tested by (name + signature) ..... :	Sean Welch	
	Approved by (+ signature) ..... :	James Klienke	
[ ]	**Testing Procedure: TMP**		
	Tested by (name + signature) ..... :		
	Approved by (+ signature) ..... :		
	Testing location / address..... :		
[ ]	**Testing Procedure: WMT**		
	Tested by (name + signature) ..... :		
	Witnessed by (+ signature)..... :		
	Approved by (+ signature) ..... :		
	Testing location / address..... :		
[ ]	**Testing Procedure: SMT**		
	Tested by (name + signature) ..... :		
	Approved by (+ signature) ..... :		
	Supervised by (+ signature) ..... :		
	Testing location / address..... :		
[ ]	**Testing Procedure: RMT**		
	Tested by (name + signature) ..... :		
	Approved by (+ signature) ..... :		
	Supervised by (+ signature) ..... :		
	Testing location / address..... :		

Summary of Testing:
Unless otherwise indicated, all tests were conducted at Underwriters Laboratories Inc. 3550 Labore Road, Suite 1, Vadnais Heights, MN, 55110, USA.

Tests performed (name of test and test clause)	Testing location / Comments
End Product Reference Page	
Input: Single-Phase (1.6.2)	
Capacitance Discharge (2.1.1.7)	
Protective Bonding II (2.6.3.4, 2.6.1)	
Strain Relief (3.2.6, 4.2.1, 4.2.7)	
Stability (4.1)	
Steady Force (4.2.1 - 4.2.4)	
Impact (4.2.5, 4.2.1)	Test conducted at UL's Northbrook, IL facillity as part of IP66 outdoor evaluation
Stress Relief (4.2.7, 4.2.1)	
Heating (4.5.1, 1.4.12, 1.4.13)	
Touch Current (Single-Phase; TN/TT System) (5.1, Annex D)	
Electric Strength (5.2.2)	

Summary of Compliance with National Differences:

AR, AT, AU, BE, CA, CH, CN, CZ, DE, DK, ES, EU, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KE, KR, MY, NL, NZ, PL, PT, SG, SI, SK, US

Copy of Marking Plate - Refer to Enclosure titled Marking Plate for copy.

Test item particulars :	
Equipment mobility .....:	movable
Operating condition .....:	continuous
Mains supply tolerance (%) .....:	N/A
Tested for IT power systems .....:	No
IT testing, phase-phase voltage (V) .....:	N/A
Class of equipment .....:	Class I (earthed)
Mass of equipment (kg) .....:	1.8 Kg
Protection against ingress of water .....:	IP66
Possible test case verdicts:	
- test case does not apply to the test object .....:	N / A
- test object does meet the requirement .....:	P(Pass)
- test object does not meet the requirement .....:	F(Fail)
Testing:	
Date(s) of receipt of test item .....:	2008-05-10, 2008-06-03
Date(s) of Performance of tests .....:	2008-05-16, 2008-05-30, 2008-06-25, 2008-06-27, 2008-06-30

General remarks:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing testing laboratory.

"(see Enclosure #)" refers to additional information appended to the report.
"(see appended table)" refers to a table appended to the report.

Throughout this report a point is used as the decimal separator.

Refer to the Cover Page For Test Report for a list of all Factory Locations.

GENERAL PRODUCT INFORMATION:

Report Summary

All applicable tests according to the referenced standard(s) have been carried out.

Product Description

10/100 Ethernet to single RS232 serial port converter wireless interfaces.

Model Differences

N/A

Additional Information

N/A

Technical Considerations

The product was submitted and tested for use at the maximum ambient temperature (Tma) permitted by the manufacturer's specification of: -40°C to 60°C

The means of connection to the mains supply is: Non-detachable power cord

The product is intended for use on the following power systems: TN

The equipment disconnect device is considered to be: Plug. Manual includes the following statement: "The plug serves as a disconnect device and must be easily accessible after the device is installed."

The following are available from the Applicant upon request: Specific data sheets for LEDs that are used for indicating purposes and assumed to be inherently Class 1 operating in the 400 - 700 nm wavelength range., Installation (Safety) Instructions / Manual

Manufacturer assumes responsibility for providing manuals and markings in the official language of the country in which the equipment is installed.

Device does not employ TNV circuits, batteries or laser devices.

The product was additionally evaluated to the requirements of UL60950-22 and IEC 60950 22 : 2005 (1st Edition). Separate IEC 60950 22 : 2005 (1st Edition) Test Report is attached to this Test Record. See Miscellaneous enclosure for of UL60950-22 and IEC 60950 22 : 2005 (1st Edition) report.

This Report does not include the investigation of the power supply. A test report or test data for the power supply may be required with this CB Test Report when submitting to another National Certification Body (NCB) for obtaining certification at the national level. Only having the License contained in Enclosure Licenses may be insufficient.

The manufacturer's maximum recommended ambient (Tma) is 60 °C. See the Supplementary Information to Table 4.5 for further details.

The ConnectPort Nema X4, Model 50001344-XX was evaluated for an altitude of up to 2000 meters only.

This report does not imply in no way indicates that the devices covered in this report have been evaluated or tested for use in a Hazardous Locations as defined by the National Electrice Code (NEC) or any other country code.

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

1	**GENERAL**		Pass
1.5	Components		Pass
1.5.1	General		Pass
	Comply with IEC 60950 or relevant component standard	(see appended table 1.5.1)	Pass
1.5.2	Evaluation and testing of components		Pass
1.5.3	Thermal controls	No thermal controls provided.	N/A
1.5.4	Transformers	Mains transformers in primary circuit previously evaluated to the requirements of IEC 60950-1 as part of separate investigation of power supply.	N/A
1.5.5	Interconnecting cables	No interconnecting cables provided as part of the equipment.	N/A
1.5.6	Capacitors in primary circuits ..... :	Capacitors in primary circuit previously evaluated to the requirements of IEC 60950-1 as part of separate investigation of power supply.	N/A
1.5.7	Double insulation or reinforced insulation bridged by components	Bridging components previously evaluated to the requirements of IEC 60950-1 as part of separate investigation of power supply	N/A
1.5.7.1	General		N/A
1.5.7.2	Bridging capacitors	Bridging components previously evaluated to the requirements of IEC 60950-1 as part of separate investigation of power supply	N/A
1.5.7.3	Bridging resistors	Bridging components previously evaluated to the requirements of IEC 60950-1 as part of separate investigation of power supply	N/A
1.5.7.4	Accessible parts		N/A
1.5.8	Components in equipment for IT power systems	Equipment not intended for IT power systems.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
1.6	**Power interface**		Pass
1.6.1	AC power distribution systems		Pass
1.6.2	Input current	See appended Table 1.6.2	Pass
1.6.3	Voltage limit of hand-held equipment	Equipment is not hand-held.	N/A
1.6.4	Neutral conductor		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

1.7	**Marking and instructions**		Pass
1.7.1	Power rating		Pass
	Rated voltage(s) or voltage range(s) (V) ..... :	100 - 240 Vac,	Pass
	Symbol for nature of supply, for d.c. only ..... :	Equipment is not d.c. rated	N/A
	Rated frequency or rated frequency range (Hz).... :		N/A
	Rated current (mA or A)..... :	0.24 A	Pass
	Manufacturer's name or trademark or identification mark ..... :	Digi International Inc.	Pass
	Type/model or type reference..... :	Digi ConnectPort X4, P/N 50001544-xx	Pass
	Symbol for Class II equipment only ..... :	Class I equipment.	N/A
	Other symbols..... :	None provided.	N/A
	Certification marks ..... :	UL, c-UL	Pass
1.7.2	Safety instructions	Evaluated English only. Manufacturer assumes responsibility of providing manuals and markings in the official language of the country in which the equipment is installed. See Miscellaneous Enclosure for manufacturer's letter of assurance.	Pass
1.7.3	Short duty cycles	Equipment intended for continuous operation.	N/A
1.7.4	Supply voltage adjustment..... :	Auto ranging	N/A
1.7.5	Power outlets on the equipment ..... :	No power outlets provided.	N/A
1.7.6	Fuse identification..... :	Fuse provided in Line of certified power supply.	N/A
1.7.7	Wiring terminals		N/A
1.7.7.1	Protective earthing and bonding terminals ..... :	No protective earthing terminal provided. Enclosure is thermoplastic and no exposed metal parts that are likely to become energized.	N/A
1.7.7.2	Terminal for a.c. mains supply conductors	Equipment is not permanently connected and does not employ a non-detachable supply cord.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
1.7.7.3	Terminals for d.c. mains supply conductors	Not a d.c. operated device.	N/A
1.7.8	Controls and indicators	No switches, controls, or indicators affecting safety are provided.	N/A
1.7.8.1	Identification, location and marking ..... :	No controls, switches, or indicators affecting safety are provided or required.	N/A
1.7.8.2	Colours..... :	No indicators, switches or controls affecting safety provided or required.	N/A
1.7.8.3	Symbols according to IEC 60417 ..... :	No symbols on controls affecting safety provided.	N/A
1.7.8.4	Markings using figures..... :	No markings using figures provided.	N/A
1.7.9	Isolation of multiple power sources ..... :	One power source.	N/A
1.7.10	IT power distribution systems	Equipment not intended for IT power systems.	N/A
1.7.11	Thermostats and other regulating devices	No thermostats or similar regulating devices provided.	N/A
1.7.12	Language..... :	Evaluated English only. Manufacturer assumes responsibility of providing manuals and markings in the official language of the country in which the equipment is installed. See Miscellaneous Enclosure for manufacturer's letter of assurance.	-
1.7.13	Durability		Pass
1.7.14	Removable parts		Pass
1.7.15	Replaceable batteries	No batteries provided.	N/A
	Language..... :		-
1.7.16	Operator access with a tool ..... :	No hazard in operator access area.	N/A
1.7.17	Equipment for restricted access locations..... :	Equipment not intended to be installed in restricted access locations.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

2	**PROTECTION FROM HAZARDS**		Pass
2.1	Protection from electric shock and energy hazards		Pass
2.1.1	Protection in operator access areas		Pass
2.1.1.1	Access to energized parts		Pass
	Test by inspection..... :	Inspection	Pass
	Test with test finger..... :	The test finger was unable to contact bare hazardous parts, basic insulation, or ELV circuits. Figure 2A test finger	Pass
	Test with test pin..... :	The test pin was unable to contact bare hazardous parts. Figure 2 B test pin	Pass
	Test with test probe ..... :	No TNV circuits or batteries.	N/A
2.1.1.2	Battery compartments..... :	No battery compartments provided.	N/A
2.1.1.3	Access to ELV wiring	No internal wiring at ELV.	N/A
	Working voltage (V); minimum distance (mm) through insulation ..... :		-
2.1.1.4	Access to hazardous voltage circuit wiring	None Provided.	N/A
2.1.1.5	Energy hazards..... :	The output of the power supply is not an energy hazard.	Pass
2.1.1.6	Manual controls	No shafts or knobs, etc. at ELV, TNV or hazardous voltage.	N/A
2.1.1.7	Discharge of capacitors in equipment		Pass
	Time-constant (s); measured voltage (V) ..... :	Initial voltage: 384 V peak. Measured 24 V peak after 1 second.	-
2.1.2	Protection in service access areas		Pass
2.1.3	Protection in restricted access locations	Equipment not intended to be installed in restricted access locations.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

2.2	**SELV circuits**		Pass
2.2.1	General requirements	Outputs of Certified power supply are SELV.	Pass
2.2.2	Voltages under normal conditions (V) ..... :	Outputs of Certified power supply are SELV.	Pass
2.2.3	Voltages under fault conditions (V)..... :	Outputs of Certified power supply are SELV.	Pass
2.2.3.1	Separation by double insulation or reinforced insulation (method 1)	Separation provided by Certified external power supply.	N/A
2.2.3.2	Separation by earthed screen (method 2)	Method 1 used.	N/A
2.2.3.3	Protection by earthing of the SELV circuit (method 3)	Method 1 used.	N/A
2.2.4	Connection of SELV circuits to other circuits..... :	SELV circuits are only connected to other SELV circuits. SELV circuit and all interconnected circuits separated by double or reinforced insulation, which is to be provided by Certified power supply .	Pass

2.3	**TNV circuits**		N/A
2.3.1	Limits		N/A
	Type of TNV circuits ..... :	No TNV circuits.	-
2.3.2	Separation from other circuits and from accessible parts		N/A
	Insulation employed..... :		-
2.3.3	Separation from hazardous voltages		N/A
	Insulation employed..... :		-
2.3.4	Connection of TNV circuits to other circuits		N/A
	Insulation employed..... :		-
2.3.5	Test for operating voltages generated externally		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
2.4	**Limited current circuits**		N/A
2.4.1	General requirements	No limited current circuits provided.	N/A
2.4.2	Limit values		N/A
	Frequency (Hz) ..... :		-
	Measured current (mA) ..... :		-
	Measured voltage (V) ..... :		-
	Measured capacitance (mF) ..... :		-
2.4.3	Connection of limited current circuits to other circuits		N/A
2.5	**Limited power sources**		N/A
	Inherently limited output	No limited power circuits provided.	N/A
	Impedance limited output		N/A
	Overcurrent protective device limited output		N/A
	Regulating network limited output under normal operating and single fault condition		N/A
	Regulating network limited output under normal operating conditions and overcurrent protective device limited output under single fault condition		N/A
	Output voltage (V), output current (A), apparent power (VA): ..... :		-
	Current rating of overcurrent protective device (A) :		-

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

2.6	**Provisions for earthing and bonding**		N/A
2.6.1	Protective earthing	No protective earthing required. Enclosure is thermoplastic and no exposed metal parts that are likely to become energized.	N/A
2.6.2	Functional earthing		N/A
2.6.3	Protective earthing and protective bonding conductors	Enclosure is thermoplastic and no exposed metal parts that are likely to become energized.	N/A
2.6.3.1	General		N/A
2.6.3.2	Size of protective earthing conductors		N/A
	Rated current (A), cross-sectional area (mm2), AWG .....:		-
2.6.3.3	Size of protective bonding conductors		N/A
	Rated current (A), cross-sectional area (mm2), AWG .....:		-
2.6.3.4	Resistance (Ohm) of earthing conductors and their terminations, test current (A) .....:		N/A
2.6.3.5	Colour of insulation.....:		N/A
2.6.4	Terminals		N/A
2.6.4.1	General		N/A
2.6.4.2	Protective earthing and bonding terminals		N/A
	Rated current (A), type and nominal thread diameter (mm) .....:		-
2.6.4.3	Separation of the protective earthing conductor from protective bonding conductors		N/A
2.6.5	Integrity of protective earthing		N/A
2.6.5.1	Interconnection of equipment		N/A
2.6.5.2	Components in protective earthing conductors and protective bonding conductors		N/A
2.6.5.3	Disconnection of protective earth		N/A
2.6.5.4	Parts that can be removed by an operator		N/A
2.6.5.5	Parts removed during servicing	No parts removable by operator.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
2.6.5.6	Corrosion resistance		N/A
2.6.5.7	Screws for protective bonding		N/A
2.6.5.8	Reliance on telecommunication network or cable distribution system		N/A
2.7	**Overcurrent and earth fault protection in primary circuits**		Pass
2.7.1	Basic requirements		Pass
	Instructions when protection relies on building installation	Equipment is not pluggable Type B or permanently connected.	N/A
2.7.2	Faults not covered in 5.3	Protection from faults not covered in Sub-Clause 5.3 are provided by installation.	Pass
2.7.3	Short-circuit backup protection	Equipment is pluggable Type A. Building installation provides short circuit protection.	Pass
2.7.4	Number and location of protective devices..... :	One fuse located in Line of Certified power supply. No additional primary circuit fuses provided.	Pass
2.7.5	Protection by several devices	No protective device in more than one pole.	N/A
2.7.6	Warning to service personnel ..... :	No neutral fusing and no parts remain energized after operation of the protective device.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

2.8	**Safety interlocks**		N/A
2.8.1	General principles	No safety interlocks provided.	N/A
2.8.2	Protection requirements		N/A
2.8.3	Inadvertent reactivation		N/A
2.8.4	Fail-safe operation		N/A
2.8.5	Moving parts		N/A
2.8.6	Overriding		N/A
2.8.7	Switches and relays		N/A
2.8.7.1	Contact gaps (mm) ..... :		N/A
2.8.7.2	Overload test		N/A
2.8.7.3	Endurance test		N/A
2.8.7.4	Electric strength test		N/A
2.8.8	Mechanical actuators		N/A

2.9	**Electrical insulation**		N/A
2.9.1	Properties of insulating materials	Insulating materials previously evaluated as part of separate investigation of Certified power supply.	N/A
2.9.2	Humidity conditioning		N/A
	Humidity (%) ..... :		-
	Temperature (°C)..... :		-
2.9.3	Grade of insulation		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

2.10	**Clearances, creepage distances and distances through insulation**		Pass
2.10.1	General		Pass
2.10.2	Determination of working voltage		Pass
2.10.3	Clearances	See Sub-Clause 5.3.4 and appended table 2.10.3 and 2.10.4.	Pass
2.10.3.1	General		Pass
2.10.3.2	Clearances in primary circuit	(see appended table 2.10.3 and 2.10.4)	N/A
2.10.3.3	Clearances in secondary circuits	See Sub-Clause 5.3.4 and appended table 2.10.3 and 2.10.4.	Pass
2.10.3.4	Measurement of transient voltage levels	Test deemed not necessary.	N/A
2.10.4	Creepage distances	See Sub-Clause 5.3.4 and appended table 2.10.3 and 2.10.4.	Pass
	CTI tests..... :	Material group IIIb.	-
2.10.5	Solid insulation		N/A
2.10.5.1	Minimum distance through insulation		N/A
2.10.5.2	Thin sheet material	None provided.	N/A
	Number of layers (pcs) ..... :		-
	Electric strength test ..... :		-
2.10.5.3	Printed boards	No supplementary or reinforced insulation on printed wiring boards.	N/A
	Distance through insulation		N/A
	Electric strength test for thin sheet insulating material ..... :		-
	Number of layers (pcs) ..... :		N/A
2.10.5.4	Wound components		N/A
	Number of layers (pcs) ..... :		N/A
	Two wires in contact inside wound component; angle between 45° and 90° ..... :		N/A
2.10.6	Coated printed boards	No coated printed boards provided.	N/A
2.10.6.1	General		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
2.10.6.2	Sample preparation and preliminary inspection		N/A
2.10.6.3	Thermal cycling		N/A
2.10.6.4	Thermal ageing (°C) ..... :		N/A
2.10.6.5	Electric strength test ..... :		-
2.10.6.6	Abrasion resistance test		N/A
	Electric strength test ..... :		-
2.10.7	Enclosed and sealed parts ..... :	No enclosed or sealed parts.	N/A
	Temperature T1=T2 = Tma - Tamb +10K (°C)..... :		N/A
2.10.8	Spacings filled by insulating compound..... :	No spacing filled by insulating compound.	N/A
	Electric strength test ..... :		-
2.10.9	Component external terminations	None provided.	N/A
2.10.10	Insulation with varying dimensions	No insulation with varying dimensions.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
3	**WIRING, CONNECTIONS AND SUPPLY**		Pass
3.1	General		Pass
3.1.1	Current rating and overcurrent protection		Pass
3.1.2	Protection against mechanical damage		Pass
3.1.3	Securing of internal wiring		Pass
3.1.4	Insulation of conductors		Pass
3.1.5	Beads and ceramic insulators	No beads or ceramic insulators provided.	N/A
3.1.6	Screws for electrical contact pressure	None provided.	N/A
3.1.7	Insulating materials in electrical connections	The equipment does not have any electrical connections that rely on insulating material for adequate contact pressure.	N/A
3.1.8	Self-tapping and spaced thread screws	Thread-cutting or space thread screws are not used for electrical connections.	N/A
3.1.9	Termination of conductors		Pass
	10 N pull test		Pass
3.1.10	Sleeving on wiring		Pass

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

3.2	**Connection to an a.c. mains supply or a d.c. mains supply**		Pass
3.2.1	Means of connection		Pass
3.2.1.1	Connection to an a.c. mains supply	Non-detachable power cord.	Pass
3.2.1.2	Connection to a d.c. mains supply	Not intended for connection to d.c. mains supply.	N/A
3.2.2	Multiple supply connections	Only one supply connection.	N/A
3.2.3	Permanently connected equipment	Equipment is not permanently connected.	N/A
	Number of conductors, diameter (mm) of cable and conduits.....:		-
3.2.4	Appliance inlets		Pass
3.2.5	Power supply cords		Pass
3.2.5.1	AC power supply cords		Pass
	Type.....:	SJTW	-
	Rated current (A), cross-sectional area (mm²), AWG .....:	A, 0.824mm², 18 AWG	-
3.2.5.2	DC power supply cords	Not intended for connection to d.c. mains supply.	N/A
3.2.6	Cord anchorages and strain relief	Test was conducted on unit employing the U.S. supply cord and on an employing the International supply cord as described in the Critical Components Table.	Pass
	Mass of equipment (kg), pull (N) .....:	1.8 Kg, 60N	-
	Longitudinal displacement (mm).....:	1) 0.8 mm displacement for U.S. cord; 2) 0.3 mm for International supply cord	-
3.2.7	Protection against mechanical damage		Pass
3.2.8	Cord guards		N/A
	D (mm); test mass (g).....:		-
	Radius of curvature of cord (mm).....:		-
3.2.9	Supply wiring space		Pass

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

3.3	**Wiring terminals for connection of external conductors**		N/A
3.3.1	Wiring terminals	Equipment is not permanently connected.	N/A
3.3.2	Connection of non-detachable power supply cords		N/A
3.3.3	Screw terminals		N/A
3.3.4	Conductor sizes to be connected		N/A
	Rated current (A), cord/cable type, cross-sectional area (mm^2) ..... :		-
3.3.5	Wiring terminal sizes		N/A
	Rated current (A), type and nominal thread diameter (mm) ..... :		-
3.3.6	Wiring terminals design		N/A
3.3.7	Grouping of wiring terminals		N/A
3.3.8	Stranded wire		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
3.4	**Disconnection from the mains supply**		Pass
3.4.1	General requirement		Pass
3.4.2	Disconnect devices	Plug on cord serves as disconnect device. Manual includes the following statement: "The plug serves as a disconnect device and must be easily accessible after the device is installed."	Pass
3.4.3	Permanently connected equipment	Equipment is not permanently connected.	N/A
3.4.4	Parts which remain energized	No parts remain energized.	N/A
3.4.5	Switches in flexible cords	No isolating switch in the cord set.	N/A
3.4.6	Single-phase equipment and d.c. equipment		Pass
3.4.7	Three-phase equipment	Equipment is not three-phase.	N/A
3.4.8	Switches as disconnect devices		N/A
3.4.9	Plugs as disconnect devices		N/A
3.4.10	Interconnected equipment		N/A
3.4.11	Multiple power sources	Only one supply connection.	N/A
3.5	**Interconnection of equipment**		Pass
3.5.1	General requirements		Pass
3.5.2	Types of interconnection circuits .....:	SELV to SELV only	Pass
3.5.3	ELV circuits as interconnection circuits	No ELV circuits provided.	N/A
4	**PHYSICAL REQUIREMENTS**		Pass
4.1	Stability		Pass
	Angle of 10°		Pass
	Test: force (N) .....:		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

4.2	**Mechanical strength**		Pass
4.2.1	General		Pass
4.2.2	Steady force test, 10 N		N/A
4.2.3	Steady force test, 30 N		Pass
4.2.4	Steady force test, 250 N		Pass
4.2.5	Impact test	Impact Test conducted as part of outdoor use evaluation, see Miscellaneous enclosure for details.	Pass
	Fall test		Pass
	Swing test	Fall test conducted.	N/A
4.2.6	Drop test	Equipment is not hand-held.	N/A
4.2.7	Stress relief test	Enclosure tested at 80°C, (77°C required).	Pass
4.2.8	Cathode ray tubes	Equipment does not employ a CRT.	N/A
	Picture tube separately certified ..... :		N/A
4.2.9	High pressure lamps	No high pressure lamps provided.	N/A
4.2.10	Wall or ceiling mounted equipment; force (N) ..... :	Equipment is not intended to be wall or ceiling mounted.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

4.3	**Design and construction**		Pass
4.3.1	Edges and corners		Pass
4.3.2	Handles and manual controls; force (N) ..... :	No handles or manual controls provided.	N/A
4.3.3	Adjustable controls	No adjustable controls provided.	N/A
4.3.4	Securing of parts		Pass
4.3.5	Connection of plugs and sockets	None provided	N/A
4.3.6	Direct plug-in equipment	Equipment is not direct plug-in.	N/A
	Dimensions (mm) of mains plug for direct plug-in . :	Equipment is not direct plug-in.	N/A
	Torque and pull test of mains plug for direct plug-in; torque (Nm); pull (N) ..... :	Equipment is not direct plug-in.	N/A
4.3.7	Heating elements in earthed equipment	No heating elements provided.	N/A
4.3.8	Batteries	No batteries provided.	N/A
4.3.9	Oil and grease	No oil or grease provided.	N/A
4.3.10	Dust, powders, liquids and gases	Equipment does not produce dust or employ powders, liquids or gases.	N/A
4.3.11	Containers for liquids or gases	No liquids or gases provided.	N/A
4.3.12	Flammable liquids ..... :	No flammable liquids provided.	N/A
	Quantity of liquid (l) ..... :		N/A
	Flash point (°C) ..... :		N/A
4.3.13	Radiation; type of radiation	No radiation produced.	Pass
4.3.13.1	General		Pass
4.3.13.2	Ionizing radiation	No radiation produced.	N/A
	Measured radiation (pA/kg) ..... :		-
	Measured high-voltage (kV) ..... :		-
	Measured focus voltage (kV) ..... :		-
	CRT markings ..... :		-
4.3.13.3	Effect of ultraviolet (UV) radiation on materials		N/A
	Part, property, retention after test, flammability classification ..... :		N/A
4.3.13.4	Human exposure to ultraviolet (UV) radiation..... :		N/A
4.3.13.5	Laser (including LEDs)	The product covered by this	Pass

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
		report employs low-power indicating LEDs. The product was not evaluated to IEC 60825. See Miscellaneous Enclosure for manufacturer's LED specifications. LEDs used for indicating purposes are Class 1 devices and operate in the range of 400-710 nm wavelength. Additional testing may be required based on auditing agency's discretion.	
	Laser class..... :	The product covered by this report employs low-power indicating LEDs. The product was not evaluated to IEC 60825. See Miscellaneous Enclosure for manufacturer's LED specifications. LEDs used for indicating purposes are Class 1 devices and operate in the range of 400-710 nm wavelength. Additional testing may be required based on auditing agency's discretion.	-
4.3.13.6	Other types ..... :		N/A
4.4	**Protection against hazardous moving parts**		N/A
4.4.1	General	No moving parts provided.	N/A
4.4.2	Protection in operator access areas		N/A
4.4.3	Protection in restricted access locations		N/A
4.4.4	Protection in service access areas		N/A
4.5	**Thermal requirements**		Pass
4.5.1	Maximum temperatures		Pass
	Normal load condition per Annex L ..... :	Passing data in loop back.	Pass
4.5.2	Resistance to abnormal heat		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

4.6	**Openings in enclosures**		N/A
4.6.1	Top and side openings	No unused openings provided.	N/A
	Dimensions (mm)..... :		-
4.6.2	Bottoms of fire enclosures		N/A
	Construction of the bottom..... :	No unused bottom openings	-
4.6.3	Doors or covers in fire enclosures		N/A
4.6.4	Openings in transportable equipment	Equipment is not transportable.	N/A
4.6.5	Adhesives for constructional purposes	No adhesives provided.	N/A
	Conditioning temperature (°C)/time (weeks) ..... :		-

4.7	**Resistance to fire**		Pass
4.7.1	Reducing the risk of ignition and spread of flame		Pass
	Method 1, selection and application of components wiring and materials		N/A
	Method 2, application of all of simulated fault condition tests	Method 1 used.	N/A
4.7.2	Conditions for a fire enclosure		Pass
4.7.2.1	Parts requiring a fire enclosure		Pass
4.7.2.2	Parts not requiring a fire enclosure		Pass
4.7.3	Materials		Pass
4.7.3.1	General		Pass
4.7.3.2	Materials for fire enclosures	Fire enclosure is Polycarbonate 3.0 mm thick rated V5.	Pass
4.7.3.3	Materials for components and other parts outside fire enclosures		Pass
4.7.3.4	Materials for components and other parts inside fire enclosures	All internal materials are rated V-2 or better or are mounted on a PWB rated V-1 or better	Pass
4.7.3.5	Materials for air filter assemblies	No air filter assemblies provided.	N/A
4.7.3.6	Materials used in high-voltage components	No high voltage components provided.	N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

5	**ELECTRICAL REQUIREMENTS AND SIMULATED ABNORMAL CONDITIONS**		Pass
5.1	Touch current and protective conductor current		Pass
5.1.1	General		Pass
5.1.2	Equipment under test (EUT)		Pass
5.1.3	Test circuit	Single-phase equipment, Figure 5A.	Pass
5.1.4	Application of measuring instrument		N/A
5.1.5	Test procedure		Pass
5.1.6	Test measurements		Pass
	Test voltage (V) ..... :	264 V ac, 60 Hz	-
	Measured touch current (mA) ..... :	0.36 mA	-
	Max. allowed touch current (mA) ..... :	3.5 mA	-
	Measured protective conductor current (mA) ..... :	0.0 mA	-
	Max. allowed protective conductor current (mA) ... :	0.25 mA	-
5.1.7	Equipment with touch current exceeding 3.5 mA .. :	Touch current does not exceed 3.5 mA.	N/A
5.1.8	Touch currents to and from telecommunication networks and cable distribution systems and from telecommunication networks	No TNV circuits	N/A
5.1.8.1	Limitation of the touch current to a telecommunication network and a cable distribution system		N/A
	Test voltage (V) ..... :		-
	Measured touch current (mA) ..... :		-
	Max. allowed touch current (mA) ..... :		-
5.1.8.2	Summation of touch currents from telecommunication networks ..... :		N/A

5.2	**Electric strength**		Pass
5.2.1	General	See appended Table 5.2	Pass
5.2.2	Test procedure	See appended Table 5.2	Pass

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

5.3	**Abnormal operating and fault conditions**		Pass
5.3.1	Protection against overload and abnormal operation	(See appended Table 5.3)	N/A
5.3.2	Motors	No motors provided.	N/A
5.3.3	Transformers	Transformers previously evaluated as part of separate investigation of Certified power supply.	N/A
5.3.4	Functional insulation ..... :	Method C used.	Pass
5.3.5	Electromechanical components	None provided.	N/A
5.3.6	Simulation of faults		N/A
5.3.7	Unattended equipment	No thermostats, temperature limiters, or thermal cut-outs provided.	N/A
5.3.8	Compliance criteria for abnormal operating and fault conditions		N/A

6	**CONNECTION TO TELECOMMUNICATION NETWORKS**		N/A
6.1	Protection of telecommunication network service persons, and users of other equipment connected to the network, from hazards in the equipment		N/A
6.1.1	Protection from hazardous voltages		N/A
6.1.2	Separation of the telecommunication network from earth		N/A
6.1.2.1	Requirements	No TNV circuits provided.	N/A
	Test voltage (V) ..... :		-
	Current in the test circuit (mA) ..... :		-
6.1.2.2	Exclusions ..... :		N/A

6.2	**Protection of equipment users from overvoltages on telecommunication networks**		N/A
6.2.1	Separation requirements	No TNV circuits provided.	N/A
6.2.2	Electric strength test procedure		N/A
6.2.2.1	Impulse test		N/A
6.2.2.2	Steady-state test		N/A
6.2.2.3	Compliance criteria		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

6.3	**Protection of the telecommunication wiring system from overheating**		N/A
	Max. output current (A) ..... :		-
	Current limiting method..... :		-

7	**CONNECTION TO CABLE DISTRIBUTION SYSTEMS**		N/A
7.1	Protection of cable distribution system service persons, and users of other equipment connected to the system, from hazardous voltages in the equipment		N/A
7.2	Protection of equipment users from overvoltages on the cable distribution system	None provided.	N/A
7.3	Insulation between primary circuits and cable distribution systems		N/A
7.3.1	General		N/A
7.3.2	Voltage surge test		N/A
7.3.3	Impulse test		N/A

A	**Annex A, TESTS FOR RESISTANCE TO HEAT AND FIRE**		N/A
A.1	Flammability test for fire enclosures of movable equipment having a total mass exceeding 18 kg, and of stationary equipment (see 4.7.3.2)		N/A
A.1.1	Samples..... :		-
	Wall thickness (mm) ..... :		-
A.1.2	Conditioning of samples; temperature (°C) ..... :		N/A
A.1.3	Mounting of samples..... :		N/A
A.1.4	Test flame		N/A
A.1.5	Test procedure		N/A
A.1.6	Compliance criteria		N/A
	Sample 1 burning time (s)..... :		-
	Sample 2 burning time (s)..... :		-
	Sample 3 burning time (s)..... :		-

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

A.2	**Flammability test for fire enclosures of movable equipment having a total mass not exceeding 18 kg, and for material and components located inside fire enclosures (see 4.7.3.2 and 4.7.3.4)**		N/A
A.2.1	Samples, material ..... :		-
	Wall thickness (mm) ..... :		-
A.2.2	Conditioning of samples		N/A
A.2.3	Mounting of samples		N/A
A.2.4	Test flame		N/A
A.2.5	Test procedure		N/A
A.2.6	Compliance criteria		N/A
	Sample 1 burning time (s)..... :		-
	Sample 2 burning time (s)..... :		-
	Sample 3 burning time (s)..... :		-
A.2.7	Alternative test acc. to IEC 60695-2-2, cl. 4, 8		N/A
	Sample 1 burning time (s)..... :		-
	Sample 2 burning time (s)..... :		-
	Sample 3 burning time (s)..... :		-

A.3	**Hot flaming oil test (see 4.6.2)**		N/A
A.3.1	Mounting of samples		N/A
A.3.2	Test procedure		N/A
A.3.3	Compliance criterion		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

B	**Annex B, MOTOR TESTS UNDER ABNORMAL CONDITIONS(see 4.7.2.2 and 5.3.2)**		N/A
B.1	General requirements	No motors provided.	N/A
	Position ..... :		-
	Manufacturer ..... :		-
	Type ..... :		-
	Rated values ..... :		-
B.2	Test conditions		N/A
B.3	Maximum temperatures		N/A
B.4	Running overload test		N/A
B.5	Locked-rotor overload test		N/A
	Test duration (days) ..... :		-
	Electric strength test: test voltage (V) ..... :		-
B.6	Running overload test for d.c. motors in secondary circuits		N/A
B.7	Locked-rotor overload test for d.c. motors in secondary circuits		N/A
B.7.1	Test procedure		N/A
B.7.2	Alternative test procedure; test time (h) ..... :		N/A
B.7.3	Electric strength test		N/A
B.8	Test for motors with capacitors		N/A
B.9	Test for three-phase motors		N/A
B.10	Test for series motors		N/A
	Operating voltage (V) ..... :		-

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
C	**Annex C, TRANSFORMERS (see 1.5.4 and 5.3.3)**		N/A
	Position ..... :	None provided.	-
	Manufacturer ..... :		-
	Type ..... :		-
	Rated values ..... :		-
	Method of protection ..... :		-
C.1	Overload test		N/A
C.2	Insulation		N/A
	Protection from displacement of windings ..... :		N/A
D	**Annex D, MEASURING INSTRUMENTS FOR TOUCH-CURRENT TESTS**		N/A
D.1	Measuring instrument		N/A
D.2	Alternative measuring instrument		N/A
E	**Annex E, TEMPERATURE RISE OF A WINDING**		N/A
F	**Annex F, MEASUREMENT OF CLEARANCES AND CREEPAGE DISTANCES (see 2.10)**		Pass

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

G	**Annex G, ALTERNATIVE METHOD FOR DETERMINING MINIMUM CLEARANCES**		Pass
G.1	Summary of the procedure for determining minimum clearances	Method C of 5.3.4 used. Functional insulation only	Pass
G.2	Determination of mains transient voltage (V)		N/A
G.2.1	AC mains supply		N/A
G.2.2	DC mains supply		N/A
G.3	Determination of telecommunication network transient voltage (V) :.....:		N/A
G.4	Determination of required withstand voltage (V) ...:		N/A
G.5	Measurement of transient levels (V).....:		N/A
G.6	Determination of minimum clearances .....:		N/A

H	**ANNEX H, IONIZING RADIATION (see 4.3.13)**		N/A

J	**Annex J, TABLE OF ELECTROCHEMICAL POTENTIALS (see 2.6.5.6)**		N/A
	Metal used .....:	No protective earthing. Enclosure is thermoplastic and no explosed metal parts likely to become energized.	-

K	**ANNEX K, THERMAL CONTROLS (see 1.5.3 and 5.3.7)**		N/A
K.1	Making and breaking capacity	None provided.	N/A
K.2	Thermostat reliability; operating voltage (V).....:		N/A
K.3	Thermostat endurance test; operating voltage (V) :		N/A
K.4	Temperature limiter endurance; operating voltage (V) .....:		N/A
K.5	Thermal cut-out reliability		N/A
K.6	Stability of operation		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

L	**Annex L, NORMAL LOAD CONDITIONS FOR SOME TYPES OF ELECTRICAL BUSINESS EQUIPMENT (see 1.2.2.1 and 4.5.1)**		Pass
L.1	Typewriters		N/A
L.2	Adding machines and cash registers		N/A
L.3	Erasers		N/A
L.4	Pencil sharpeners		N/A
L.5	Duplicators and copy machines		N/A
L.6	Motor-operated files		N/A
L.7	Other business equipment	Passing data in loop back.	Pass

M	**Annex M, CRITERIA FOR TELEPHONE RINGING SIGNALS (see 2.3.1)**		N/A
M.1	Introduction		N/A
M.2	Method A	No ringing signals generated.	N/A
M.3	Method B		N/A
M.3.1	Ringing signal		N/A
M.3.1.1	Frequency (Hz) ..... :		-
M.3.1.2	Voltage (V) ..... :		-
M.3.1.3	Cadence; time (s), voltage (V) ..... :		-
M.3.1.4	Single fault current (mA) ..... :		-
M.3.2	Tripping device and monitoring voltage ..... :		N/A
M.3.2.1	Conditions for use of a tripping device or a monitoring voltage		N/A
M.3.2.2	Tripping device		N/A
M.3.2.3	Monitoring voltage (V) ..... :		N/A

N	**Annex N, IMPULSE TEST GENERATORS (see 2.10.3.4, 6.2.2.1, 7.3.2 and clause G.5)**		N/A
N.1	ITU-T impulse test generators		N/A
N.2	IEC 60065 impulse test generator		N/A

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict
P	**Annex P, NORMATIVE REFERENCES**		Pass
Q	**Annex Q, BIBLIOGRAPHY**		Pass
R	**Annex R, EXAMPLES OF REQUIREMENTS FOR QUALITY CONTROL PROGRAMMES**		N/A
R.1	Minimum separation distances for unpopulated coated printed boards (see 2.10.6)		N/A
R.2	Reduced clearances (see 2.10.3)		N/A
S	**Annex S, PROCEDURE FOR IMPULSE TESTING (see 6.2.2.3)**		N/A
S.1	Test equipment		N/A
S.2	Test procedure		N/A
S.3	Examples of waveforms during impulse testing		N/A
T	**Annex T, GUIDANCE ON PROTECTION AGAINST INGRESS OF WATER (see 1.1.2)**		Pass
	..... :	IP66	-
U	**Annex U, INSULATED WINDING WIRES FOR USE WITHOUT INTERLEAVED INSULATION (see 2.10.5.4)**		N/A
	..... :	No triple insulated wire provided.	-

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

1.5.1	**TABLE: list of critical components**				Pass
object/part No.	manufacturer/ trademark	type/model	technical data	standard	mark(s) of conformity[1])
Enclosure	Hoffman	Q24169PCDCC	Polycarbonate	Evaluated in the end product to IEC 60950-1.	UL, c-UL, -
Power Supply	Bobbintron Electronics	AD0243-24	Input: 100 - 240 Vac, 50 - 60 Hz, 0.7 A Output: 24 Vdc / 1.0 A Insulation of Transformer T1 winding is Class B. Mounted on 4.5 mm high standoffs	IEC60950-1:2001 1st Edition also evaluated to IEC 60950-1.	UL, c-UL, CB
Power Supply Internal Cover	Various	Various	Metal, 0.6 mm Thick, provided with 123, 4.5 mm diameter holes over the entire cover.	Evaluated in the end product to IEC 60950-1.	-, -
PCB Board	Various	Various	V0, 130 C minimum.	UL 796. Evaluated in the end product to IEC 60950-1.	UL, c-UL, -
PCI Express Mini Card	Digi International Inc.	50001380-xx	3.0 - 3.6 Vdc	IEC 60950-1	UL, c-UL, CB
Strain Relief	Hummel Metall-UND Kunststofftechnik GMBH	HSK-K	Suitable for cord for which it is applied to.	Evaluated in the end product to IEC 60950-1.	UL, c-UL, -
International Power Cord	Yung Li	YP-22	Rated 250 Vac, 16 A, HO5VV-F 3 G 0.75 - 1.5 mm ², 3 conductor.	DIN VDE 0620-1 (VDE 0620-1):2005-04, additionally evaluated in the end product to IEC 60950-1.	-, VDE
Name Plate	3M	7816	Adhesive backed suitable for surface for which it is applied, for indoor and outdoor use.	UL 969 additionally evaluated in the end product to IEC 60950-1.	UL, c-UL, -

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

Ratings Label	3M	7816	Adhesive backed suitable for surface for which it is applied, for indoor and outdoor use.	UL 969 additionally evaluated in the end product to IEC 60950-1.	UL, c-UL, -
Label ink	Avery Dennsion Corp	SP-330	suitable for surface for which it is applied, for indoor and outdoor use.	UL 969 additionally evaluated in the end product to IEC 60950-1.	UL, c-UL
LED	Avago technologies	HSMF-A226-xxxxx	See enclosures Miscellaneous	Evaluated in the end product to IEC 60950-1.	-, -
[1]) an asterisk indicates a mark which assures the agreed level of surveillance					

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

1.6.2	**TABLE: electrical data (in normal conditions)**					Pass
fuse #	I rated (A)	U (V)	P (W)	I (mA)	I fuse (mA)	condition/status
N/A	N/A	90 V ac, 50 Hz	9.4	0.2	N/A	Maximum Normal Load
N/A	0.24 A	100 V ac, 50 Hz	9.3	0.2	N/A	Maximum Normal Load
N/A	0.24 A	120 V ac, 50 Hz	9.4	0.17	N/A	Maximum Normal Load
N/A	0.24 A	132 V ac, 50 Hz	9.4	0.16	N/A	Maximum Normal Load
N/A	0.24 A	200 V ac, 50 Hz	10.0	0.13	N/A	Maximum Normal Load
N/A	0.24 A	220 V ac, 50 Hz	10.0	0.12	N/A	Maximum Normal Load
N/A	0.24 A	240 V ac, 50 Hz	10.0	0.11	N/A	Maximum Normal Load
N/A	N/A	264 V ac, 50 Hz	10.0	0.11	N/A	Maximum Normal Load
N/A	N/A	90 V ac, 60 Hz	9.4	0.2	N/A	Maximum Normal Load
N/A	0.24 A	100 V ac, 60 Hz	9.3	0.19	N/A	Maximum Normal Load
N/A	0.24 A	120 V ac, 60 Hz	9.3	0.17	N/A	Maximum Normal Load
N/A	0.24 A	132 V ac, 60 Hz	9.4	0.16	N/A	Maximum Normal Load
N/A	0.24 A	200 V ac, 60 Hz	10.0	0.13	N/A	Maximum Normal Load
N/A	0.24 A	220 V ac, 60 Hz	10.0	0.12	N/A	Maximum Normal Load
N/A	0.24 A	240 V ac, 60 Hz	10.0	0.11	N/A	Maximum Normal Load
N/A	N/A	264 V ac, 60 Hz	10.0	0.11	N/A	Maximum Normal Load
supplementary information:						

2.10.3 and 2.10.4	**TABLE: clearance and creepage distance measurements**					Pass
clearance cl and creepage distance dcr at/of:	Up (V)	U r.m.s. (V)	required cl (mm)	cl (mm)	required dcr (mm)	dcr (mm)
Primary to ground traces on power supply	340	240	2.0	4.1	2.5	4.1

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

Primary to metal mounting plate	340	240	2.0	4.2	2.5	4.1
supplementary information:						
Method C of 5.3.4 for secondary spacings.						

2.10.5	**TABLE: distance through insulation measurements**				N/A
distance through insulation di at/of:		Up (V)	test voltage (V)	required di (mm)	di (mm)
-		-	-	-	-
supplementary information:					

4.5	**TABLE: temperature rise measurements**						Pass
	test voltage (V)	90 Vac, 50 Hz	90 Vac, 60 Hz	132 Vac, 60 Hz	200 Vac, 50 Hz	264 Vac, 50 Hz	—
	t1 (°C).....	21	21	21	61	61	—
	t2 (°C).....	21	21	21	61	61	—
maximum temperature T of part/at:		T (°C)					allowed Tmax (°C)
The following are located on the power supply		-	-	-	-	-	-
Transformer T1 winding (Class B)		59	51	52	91	94	110
Transformer T1 winding (Class B)		60	51	52	92	94	110
Inductor winding near C2		42	40	40	75	77	105
Capacitor C1 body		47	42	42	80	83	85
Inductor winding near C13		52	46	46	84	86	105
PWB near HS2		57	49	49	89	91	105
The following are located on The connectPort X4 NEMA		-	-	-	-	-	-
IC Xbee Series 2		46	43	44	77	77	105
Inductor L27		44	41	42	74	75	105
Capacitor body C67		41	39	39	72	72	85
TC63 Adapter module		39	37	37	71	71	105
Ethernet Switch case		37	34	35	69	69	70
Internal wiring to PWB		35	32	33	67	67	90
Enclosure probe method		32	30	30	64	64	95
The following are located on the power supply		-	-	-	-	-	-
PWB near input choke		47	43	44	80	82	105
Input wiring		36	33	34	70	71	105
PWB near bridge rectifier		60	53	54	92	94	105

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

PWB near switching transistor	58	51	52	90	92	105
Top internal enclosure	-	-	-	63	63	
Top internal enclosure	-	-	-	63	63	
Top internal enclosure	-	-	-	64	64	
Bottom internal enclosure	-	-	-	67	67	
Bottom internal enclosure	-	-	-	64	64	
Bottom internal enclosure	-	-	-	64	65	
maximum temperature T of part/at:	T (°C) #6	-	-	-	-	-
Test Voltage (V)	264 Vac, 60 Hz	-	-	-	-	-
Ambient ((C)	61	-	-	-	-	-
The following are located on the power supply	-	-	-	-	-	-
Transformer T1 winding (Class B)	93	-	-	-	-	110
Transformer T1 winding (Class B)	94	-	-	-	-	110
Inductor winding near C2	76	-	-	-	-	105
Capacitor C1 body	83	-	-	-	-	85
Inductor winding near C13	85	-	-	-	-	105
PWB near HS2	91	-	-	-	-	105
The following are located on The connectPort X4 NEMA	-	-	-	-	-	-
IC Xbee Series 2	77	-	-	-	-	105
Inductor L27	74	-	-	-	-	105
Capacitor body C67	72	-	-	-	-	85
TC63 Adapter module	71	-	-	-	-	105
Ethernet Switch case	69	-	-	-	-	70
Internal wiring to PWB	67	-	-	-	-	90
Enclosure probe method	64	-	-	-	-	95
The following are located on the power supply	-	-	-	-	-	-
PWB near input choke	82	-	-	-	-	105
Input wiring	71	-	-	-	-	105
PWB near bridge rectifier	94	-	-	-	-	105
PWB near switching transistor	92	-	-	-	-	105
Top internal enclosure	63	-	-	-	-	
Top internal enclosure	63	-	-	-	-	
Top internal enclosure	64	-	-	-	-	
Bottom internal enclosure	67	-	-	-	-	
Bottom internal enclosure	64	-	-	-	-	
Bottom internal enclosure	65	-	-	-	-	
temperature T of winding:		R_1 (Ω)	R_2 (Ω)	T (°C)	allowed Tmax (°C)	insulation class

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

supplementary information:
Maximum temperatures measured were recorded in the table above. The manufacturer's maximum recommended ambient (Tma) of 60°C was taken into consideration for compliance with Tmax as noted above.

4.5.2	**TABLE: ball pressure test of thermoplastics**		N/A
	allowed impression diameter (mm) ..... :	N/A	—
part		test temperature (°C)	impression diameter (mm)
N/A		N/A	N/A
supplementary information:			

4.7	**TABLE: resistance to fire**			Pass
part	manufacturer of material	type of material	thickness(mm)	flammability class
Enclosure	Hoffman	Polycarbonate	3.0 mm	V5
supplementary information:				
See Critical Components Table 1.5.1				

5.2	**TABLE: electric strength tests, impulse tests and voltage surge tests**		Pass
test voltage applied between:		test voltage (V) a.c./d.c.	breakdown Yes / No
Foiled cover to Primary (Foil wrapped Double insulation)		2414 V dc	No
Primary to Ground		2414Vdc	No
Primary to Secondary		4242Vdc	No
supplementary information:			

5.3	**TABLE: fault condition tests**		N/A
	ambient temperature (°C) ..... :	N/A	—
	model/type of power supply ..... :	N/A	—
	manufacturer of power supply ..... :	N/A	—
	rated markings of power supply ..... :	N/A	—

IEC 60950-1			
Clause	Requirement + Test	Result - Remark	Verdict

component No.	fault	test voltage (V)	test time	fuse No.	fuse current (A)	result
N/A						
supplementary information:						

Enclosure

National Differences

Argentina*
Australia / New Zealand
Austria**
Belgium**
China*
Czech Republic**
Denmark
Finland
France**
Germany
Greece**
Group
Hungary*
India*
Ireland*
Israel*
Italy*
Japan*
Kenya*
Korea
Malaysia*
Netherlands**
Poland*
Portugal*
Singapore*
Slovakia**
Slovenia*
Spain*
Switzerland**
USA / Canada
United Kingdom

* No National Differences Declared
** Only Group Differences

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict

Australia / New Zealand - Differences to IEC 60950-1:2001, First Edition			
1.2.12.11	POTENTIAL IGNITION SOURCE Possible fault which can starts a fire if the open-circuit voltage measured across an interruption or faulty contact exceeds a value of 50 V (peak) a.c. or d.c. and the product of the peak value of this voltage and the measured r.m.s. current under normal operating conditions exceeds 15VA. Such a faulty contact or interruption in an electrical connection includes those which may occur in conductive patterns on printed boards. Note 201: An electronic protection circuit may be used to prevent such a fault from becoming a POTENTIAL IGNITION SOURCE.		Pass
1.5.1	Add to the first paragraph: "or the relevant Australian / New Zealand Standard".		Pass
1.5.2	Add to the first and third dashed items after the words "IEC Component Standard": "or the relevant Australian / New Zealand Standard".		Pass
1.6.1	Add: AC power distribution systems classified as TT or IT are not allowed		N/A
1.7.12	Add to the first paragraph: All safety instructions and safety markings shall be in English.		Pass
3.2.5	Substitute for Table 3B: Sizes of Conductors --- Rated Current of Equipment (A) / Nominal cross-sectional area (mm²) --- 0.2 <= 3 — 0.5* 3 <= 7.5 — 0.75 7.5 <= 10 — (0.75) 1.00 10 <= 16 — (1,0) 1.5 16 <= 25 — 2.5 25 <= 32 — 4 32 <= 40 — 6 40 <= 63 — 10 63 <= 80 — 16 80 <= 100 — 25 100 <= 125 — 35 125 <= 160 — 50 160 <= 190 — 70 190 <= 230 — 95 230 <= 260 — 120		Pass

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	260 <= 300 150 300 <= 340 185 340 <= 400 240 400 <= 460 300 --- * This nominal cross-sectional area is only allowed for Class II appliances if the length of the power supply cord, measured between the point where the cord or cord guard, enters the appliance, and the entry to the plug, does not exceed 2 m (0.5 mm² three-core supply flexible cords are not permitted; see Note 2 to Table 2.17 of AS/NZS 3191).		
4.3.6	Replace the third paragraph: Equipment with a plug portion, suitable for insertion into a 10 A 3-pin flat-pin socket-outlet complying with AS/NZS 3112, shall comply with the requirements in AS/NZS 3112 for equipment with integral pins for insertion into socket-outlets.		N/A
4.3.13	For the purpose of this standard compliance with AS/NZS 2211.1 is deemed to be compliance with IEC60825.1	LEDs used for indicating purposes are Class 1 devices and operate in the range of 400-700 nm wavelength. Additional testing may be required based on auditing agency's discretion.	Pass
4.7	Add after the clause: For alternative resistance to fire tests, refer to Annex YY.		N/A
6.2.1	Replace item c) with: An SELV circuit, a TNV-2 circuit or a Limited Current Circuit provided for connection of other equipment. The requirement for separation applies whether or not this circuit is accessible.		N/A
6.2.2	Replace the first paragraph by: In Australia (not in New Zealand), compliance with 6.2.2 is checked by the tests of both 6.2.2.1 and 6.2.2.2.		N/A
6.2.2.1	Replace 6.2.2.1 with: In Australia (not in New Zealand), the electrical separation is subjected to 10 impulses of alternating polarity, using the impulse test generator of Annex N for 10/700µs impulses. The interval between successive impulses is 60 s and the initial voltage, Uc is: - for 6.2.1a): 7.0 kV for hand-held telephones and for headsets;		N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	2.5 kV for other equipment; for 6.2.1b) and 6.2.1c): 1.5 kV. NOTE 1 - The 7 kV impulse is to simulate lightning surges on typical rural and semi-rural network lines. NOTE 2 - The value of 2.5 kV for 6.2.1a) was chosen to ensure adequacy of the insulation concerned and does not necessarily simulate likely overvoltages.		
6.2.2.2	Replace the first and second paragraphs of 6.2.2.2 with: In Australia (not New Zealand), the electrical separation is subjected to an electric strength test according to 5.2.2. The a.c. test voltage is: - for 6.2.1a) 3 kV - for 6.2.1b) and 6.2.1c) 1.5 kV NOTE 1 - Where there are capacitors across the insulation under test, it is recommended that d.c. test voltages are used. NOTE 2 - The 3 kV and 1.5 kV values have been determined considering the low frequency induced voltages from the power supply distribution system.		N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
Denmark - Differences to IEC 60950-1:2001, First Edition			
1.2.4.1	Certain types of Class I appliances (see sub-clause 3.2.1.1) may be provided with plug not establishing earthing continuity when inserted into Danish socket-outlets.	See Enclosure Miscellaneous for Manufacturer's Letter of Assurance. Manufacturer assumes responsibility of providing a cord and plug that is suitable for the country in which it is installed.	Pass
1.7.2	Supply cords of Class I equipment, which is delivered without a plug, must be provided with a visible tag with the following text: "Vigtigt ! Lederen med grøn/gul isolation må kun tilsluttes en klemme mærket (IEC 417, No. 5019) eller (IEC 417, No. 5017)." If essential for the safety of the equipment, the tag must in addition be provided with a diagram, which shows the connection of the other conductors, or be provided with the following text: "For tilslutning af de øvrige ledere, se medfølgende installationsvejledning".		Fail
1.7.5	Socket-outlets for providing power to other equipment shall be in accordance with the Heavy Current Regulations, Section 107-2-D1, Standard Sheet DK 1-3a, DK 1-5a or DK 1-7a, when used on Class I equipment. For stationary equipment, the socket0outlet shall be in accordance with Standard Sheet DK 1-1b or DK 1-5a.	No socket-outlets provided.	N/A
1.7.5	Class II equipment shall not be fitted with socket-outlets for providing power to other equipment.	Class I equipment. No socket-outlets provided.	N/A
3.2.1.1	Supply cord of single-phase equipment having a rated current not exceeding 13 A shall be provided with a plug according to the Heavy Current Regulations, Section 107-2-D1. Class I equipment provided with socket-outlets with earth contact or which are intended to be used in locations where protection against indirect contact is required according to the wiring rules shall be provided with a plug in accordance with standard sheet DK 2-1a or DK 2-5a. If poly-phase equipment and single-phase	See Enclosure Miscellaneous for Manufacturer's Letter of Assurance. Manufacturer assumes responsibility of providing a cord and plug that is suitable for the country in which it is installed.	Pass

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	equipment having a rated current exceeding 13 A is provided with a supply cord with a plug, this plug shall be in accordance with the Heavy Current Regulations, Section 107-2-D1 or EN 60309-2.		

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
Finland - Differences to IEC 60950-1:2001, First Edition			
1.7.2	Class I Pluggable Equipment Type A intended for connection to other equipment or a network shall, if safety relies on connection to protective earth or if surge suppressors are connected between the network terminals and accessible parts, have a marking stating that the equipment must be connected to an earthed mains socket-outlet. The marking text shall be: "Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan"	For connection to other equipment or a network, safety does not rely on connection to protective earth and no surge suppressors are connected between the network terminals and accessible parts.	N/A
6.1.2.1	Add the following text between the first and second paragraph: If this insulation is solid, including insulation forming part of a component, it shall at least consist of either - two layers of thin sheet material, each of which shall pass the electric strength test below, or - one layer having a distance through insulation of at least 0.4 mm, which shall pass the electric strength test below. If this insulation forms part of a semiconductor component (e.g. an optocoupler), there is no distance through insulation requirement for the insulation consisting of an insulating compound completely filling the casing, so that clearances and creepage distances do not exist, if the component passes the electric strength test in accordance with the compliance clause below and in addition: - passes the tests and inspection criteria of IEC 60950-1, 2.10.8 with an electric strength test of 1.5 kV multiplied by 1.6 (the electric strength test of 2.10.7 shall be performed using 1.5 kV), and - is subject to routing testing for electric strength during manufacturing, using a test voltage of 1.5 kV. It is permitted to bridge this insulation with a capacitor complying with IEC 60384-14:1993, subclass Y2. A capacitor classified Y3 according to IEC 60384-14:1993, may bridge this insulation under the following conditions: - the insulation requirements are satisfied by having a capacitor classified Y3 as defined by IEC 60384-14, which in addition to the Y3 testing, is tested with an impulse test of 2.5 kV defined in EN	No TNV circuits provided.	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	60950-1, subclause 6.2.2.1; - the additional testing shall be performed on all the test specimens as described in IEC 60384-14; - the impulse test of 2,5 kV is to be performed before the endurance test in IEC 60384-14, in the sequence of tests as described in IEC 60384-14.		
6.1.2.2	The exclusions are applicable for permanently connected equipment and pluggable equipment type B and equipment intended to be used in a restricted access location where equipotential bonding has been applied, e.g. in a telecommunication centre, and which has provision for a permanently connected protective earthing conductor and is provided with instructions for the installation of that conductor by a service person.	No TNV circuits provided.	N/A
7.1	Requirements according to this annex, 6.1.2.1 and 6.1.2.2 apply with the term telecommunication network in 6.1.2 being replaced by the term cable distribution system.	No connections to cable distribution systems.	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
Germany - Differences to IEC 60950-1:2001, First Edition			
1.7.12	(Gesetz uber technische Arbeitsmittel (Garatesicherheitsgesetz) [Law of technical labour equipment {Equipment safety law}], of 23rd October 1992, Article 3, 3rd paragraph, 2nd sentence, together with the "Allgemeine Verwaltungsvorschrift zur Durchfuhrung des Zweiten Abschritts des Geratesicherheitsgesetzes" [General administrative regulation on the execution of the Second Section of the Equipment safety law], of 10th January 1996, article 2, the paragraph, item 2). Directions for use with rules to prevent certain hazards for (among others) maintenance of the technical labour equipment, also for imported technical labour equipment shall be written in the German language. NOTE: Of this requirement, rules for use even only by service personnel are not exempted.	Evaluated English only. Manufacturer assumes responsibility of providing manuals and markings in the official language of the country in which the equipment is installed. See Miscellaneous Enclosure for manufacturer's Letter of Assurance.	Pass
H	(Regulation on protection against hazards by X-ray,of 8th January 1987, Article 5 [operation of X-ray emission source], clauses 1 to 4) a) A licence is required by those who operate an X-ray emission source. b) A licence in accordance with Cl. 1 is not required by those who operate an X-ray emission source on which the electron acceleration voltage does not exceed 20 kV if 1) the local dose rate at a distance of 0,1 m from the surface does not exceed 1 µSv/h and 2) it is adequately indicated on the X-ray emission source that i) X-rays are generated ii) the electron acceleration voltage must not exceed the maximum value stipulated by the manufacturer or importer. c) A licence in accordance with Cl. 1 is also not required by persons who operate an X-ray emission source on which the electron acceleration voltage exceeds 20 kV if 1) the X-ray emission source has been granted a type approval and 2) it is adequately indicated on the X-ray emission source that i) X-rays are generated ii) the device stipulated by the manufacturer or importer guarantees that the maximum	None provided.	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	permissible local dose rate in accordance with the type approval is not exceeded and iii) the electron acceleration voltage must not exceed the maximum value stipulated by the manufacturer or importer. d) Furthermore, a licence in accordance with Cl. 1 is also not required by persons who operate X-ray emission sources on which the electron acceleration voltage does not exceed 30 kV if 1) the X-rays are generated only by intrinsically safe CRTs complying with Enclosure III, No. 6, 2) the values stipulated in accordance with Enclosure III, No. 6.2 are limited by technical measures and specified in the device and 3) it is adequately indicated on the X-ray emission source that the X-rays generated are adequately screened by the intrinsically safe CRT.		

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
Group - Differences to IEC 60950-1:2001, First Edition			
2.7.1	Replace the subclause as follows: Basic requirements To protect against excessive current, short-circuits and earth faults in primary circuits, protective devices shall be included either as integral parts of the equipment or as parts of the building installation, subject to the following, a), b) and c): a) except as detailed in b) and c), protective devices necessary to comply with the requirements of 5.3 shall be included as parts of the equipment; b) for components in series with the mains input to the equipment such as the supply cord, appliance coupler, r.f.i. filter and switch, short-circuit and earth fault protection may be provided by protective devices in the building installation; c) it is permitted for pluggable equipment type B or permanently connected equipment, to rely on dedicated overcurrent and short-circuit protection in the building installation, provided that the means of protection, e.g. fuses or circuit breakers, is fully specified in the installation instructions. If reliance is placed on protection in the building installation, the installation instructions shall so state, except that for pluggable equipment type A the building installation shall be regarded as providing protection in accordance with the rating of the wall socket outlet.		N/A
2.7.2	Void		N/A
2.10.2	Replace the first line "(see also 1.4.7)" by "(see also 1.4.8)".		Pass
3.2.3	Delete NOTE 1, and in table 3A delete the conduit sizes in parentheses.	Equipment is not permanently connected.	N/A
3.2.5	Replace: "60245 IEC 53" by "H05 RR-F" "60227 IEC 52" by "H03 VV-F or H03 VVH2-F" "60227 IEC 53" by "H05 VV-F or H05 VVH2-F" In table 3B, replace the first four lines by the following: Up to and including 6 0.75 [1] Over 6 up to and including 10 0.75 [2] 1.0 Over 10 up to and including 16 1.0 [3] 1.5 In the Conditions applicable to table 3B, delete the		Pass

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	words "in some countries" in condition [1]. In Note 1, delete the second sentence.		
3.3.4	In table 3D, delete the fourth line: conductor sizes for 10 to 13 A, and replace with the following: "Over 10 up to and including 16 1.5 to 2.5 1.5 to by 4" Delete the fifth line: conductor sizes for 13 to 16A.	Equipment is not permanently connected	N/A
4.3.13.6	Add the following note: NOTE - Attention is drawn to 1999/519/EC: Council Recommendation on the limitation of exposure of the general public to electromagnetic fields 0 Hz to 300 GHz. Standards taking into account this recommendation are currently under development.	Equipment does not generate electromagnetic fields.	N/A
General	Delete all the "country" notes in the reference document according to the following list: 1.5.1 Note 2 1.5.8 Note 2 1.6.1 Note 1.7.2 Note 4 1.7.12 Note 2 2.1 Note 2.2.3 Note 2.2.4 Note 2.3.2 Note 2, 7, 8 2.3.3 Note 1, 2 2.3.4 Note 2,3 2.7.1 Note 2.10.3.1 Note 4 3.2.1.1 Note 3.2.3 Note 1, 2 3.2.5.1 Note 2 4.3.6 Note 1,2 4.7.2.2 Note 4.7.3.1 Note 2 6.1.2.1 Note 6.1.2.2 Note 6.2.2 Note 6.2.2.1 Note 2 6.2.2.2 Note 7 Note 4 7.1 Note G2.1 Note 1, 2 H Note 2		Pass
H	Replace the last paragraph of this annex by: At any point 10 cm from the surface of the operator access area, the dose rate shall not exceed 1 µSv/h (0,1 mR/h) (see note). Account is taken of the background level. Replace the notes as follows: NOTE - These values appear in Directive 96/29/Euratom. Delete Note 2.	Equipment does not generate X-radiation.	N/A
P	Replace the text of this annex by: See annex ZA		Pass
Q	Replace the title of IEC 61032 by "Protection of persons and equipment by enclosures - Probes for verification". Add the following notes for the standards indicated: IEC 60127 NOTE Harmonized as EN 60127		Pass

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	(Series) (not modified) IEC 60269-2-1 NOTE Harmonized as HD 630.2.1 S4:2000 (modified) IEC 60529 NOTE Harmonized as EN 60529:1991 (not modified) IEC 61032 NOTE Harmonized as EN 61032:1998 (not modified) IEC 61140 NOTE Harmonized as EN 61140:2001 (not modified) ITU-T Recommendation K.31 NOTE in Europe, the suggested document is EN 50083-1.		

Korea - Differences to IEC 60950-1:2001, First Edition			
1.5.101	Addition: Plugs for the connection of the apparatus to the supply mains comply with the Korean requirement (KSC 8305).	Manufacturer assumes responsibility of providing a cord and plug that is suitable for the country in which it is installed. See Enclosure Miscellaneous for Manufacturer's Letter of Assurance.	N/A
7	Addition: EMC - The apparatus shall complies with the relevant CISPR standards.	See Miscellaneous Enclosure for manufacturer's letter of assurance.	Pass

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict

USA / Canada - Differences to IEC 60950-1:2001, First Edition			
1.1	Equipment able to be installed in accordance with the National Electrical Code ANSI/NFPA 70 and the Canadian Electrical Code, Part1, and when applicable, the National Electrical Safety Code, IEEE C2.		Pass
1.1.1	Equipment able to be installed in accordance with ANSI/NFPA 75 and NEC Art. 645 unless intended for use outside of computer room and provided with such instructions.	No TNV circuits.	N/A
1.1.2	Equipment in wire-line communication facilities serving high-voltage electric power stations operating at greater than 1kV are excluded.		N/A
1.1.2	Special requirements apply to equipment intended for use outdoors.	See Miscellaneous Enclosure for details on outdoor evaluation.	Pass
1.4.14	For Pluggable Equipment Type A, the protection in the installation is assumed to be 20 A.		Pass
1.5.1	All IEC standards for components identified in Annex P.1 replaced by the relevant requirements of CSA and UL component standards in Annex P.1.		Pass
1.5.1	All IEC standards for components identified in Annex P.2 alternatively satisfied by the relevant requirements of CSA and UL component standards in Annex P.2.		Pass
1.5.5	Interconnecting cables acceptable for the application regarding voltage, current, temperature, flammability, mechanical serviceability and the like.	No interconnecting cables provided.	N/A
1.5.5	For other than limited power and TNV circuits, the type of output circuit identified for output connector.	None provided.	N/A
1.5.5	External cable assemblies that exceed 3.05 m in length to be types specified in the NEC and CEC.	None provided.	N/A
1.5.5	Detachable external interconnecting cables 3.05 m or less in length and provided with equipment marked to identify the responsible organization and the designation for the cable.	None provided.	N/A
1.5.5	Building wiring and cable for use in ducts, plenums and other air handling space subject to special requirements and excluded from scope.	Not intended for use in ducts, plenums or other air handling spaces.	N/A
1.5.5	Telephone line and extension cords and the like comply with UL 1863 and CSA C22.2 No. 233.	No TNV circuits.	N/A
1.6.1.2	Equipment intended for connection to a d.c. power	Not Intended for connection to	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	(mains) distribution system is subject to special circuit classification requirements (e.g., TNV-2)	d.c. mains supply.	
1.6.1.2	Earthing of d.c. powered equipment provided.		N/A
1.7	Lamp replacement information indicated on lampholder in operator access area.	No lamps provided	N/A
1.7.1	Special marking format for equipment intended for use on a supply system with an earthed neutral and more than one phase conductor.	Equipment intended for use with one phase conductor.	N/A
1.7.1	Equipment voltage rating not higher than rating of the plug except under special conditions.		Pass
1.7.6	Special fuse replacement marking for operator accessible fuses.	No operator accessible fuses provided	N/A
1.7.7	Identification of terminal connection of the equipment earthing conductor.		N/A
1.7.7	Connectors and field wiring terminals for external Class 2 or Class 3 circuits provided with marking indicating minimum Class of wiring to be used.	No external terminals provided.	N/A
1.7.7	Marking located adjacent to terminals and visible during wiring.	No external terminals provided.	N/A
2.1.1	Screw shell of Edison-base lampholder tied to the neutral conductor.	No Lamps Provided	N/A
2.1.1.1	Bare TNV conductive parts in the interior of equipment normally protected against contact by a cover intended for occasional removal are exempt provided instructions include directions for disconnection of TNV prior to removal of the cover.	No TNV circuits.	N/A
2.3.1.b	Other telecommunication signaling systems (e.g., message waiting) than described in 2.3.1(b) are subject to M.4.		N/A
2.3.1.b	For TNV-2 and TNV-3 circuits with other than ringing signals and with voltages exceeding 42.4 Vp or 60 V d.c., the maximum current limit through a 2000 Ohm or greater resistor with loads disconnected is 7.1 mA peak or 30 mA d.c. under normal conditions.		N/A
2.3.1.b	Limits for measurements across 5000 ohm resistor in the event of a single fault are replaced after 200 ms with the limits of M.3.1.4.		N/A
2.3.2	Enamel coating on signal transformer winding wire allowed as an alternative to Basic insulation in specific telecommunication applications when subjected to special construction requirements and		N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	routine testing.		
2.3.2	In the event of a single fault, the limits of 2.2.3 apply to SELV circuits and accessible conductive parts.		Pass
2.5	Overcurrent protection device required for Class 2 and Class 3 limiting in accordance with the NEC, or for a Limited Power Source, not interchangeable with devices of higher ratings if operator replaceable.		N/A
2.6	Equipment having receptacles for output a.c. power connectors generated from an internal separately derived source have the earthed (grounded) circuit conductor suitably bonded to earth.	None provided	N/A
2.6.3.3	For Pluggable Equipment Type A, if neither a) or b) are applicable, the current rating of the circuit is taken as 20 A.		N/A
2.6.3.4	Capacity of connection between earthing terminal and parts required to be earthed subject to special conditions based on the current rating of the circuit.		N/A
2.6.3.4	Protective bonding conductors and their terminals of non-standard constructions (e.g. PWB traces) evaluated to limited short-circuit test of CSA C22.2 No.0.4.		N/A
2.6.4.1	Field wiring terminals for earthing conductors suitable for wire sizes (gauge) used in US and Canada.	No field wiring terminals	N/A
2.7.1	Data for selection of special external branch circuit overcurrent devices marked on the equipment.	None required	N/A
2.7.1	Standard supply outlets protected by overcurrent device in accordance with the NEC, and CEC, Part 1.	No standard supply outlets provided.	N/A
2.7.1	Overcurrent protection for individual transformers that distribute power to other units over branch circuit wiring.	None provided.	N/A
2.7.1	Additional requirements for overcurrent protection apply to equipment provided with panelboards.	No panelboards provided	N/A
2.7.1	Non-motor-operated equipment requiring special overcurrent protective device marked with device rating.	No special overcurrent protective devices required	N/A
2.10.5.4	Multi-layer winding wire subject to UL component wire requirements in addition to 2.10.5.4 and Annex U.	Previously evaluated as part of separate investigation of Certified power supply.	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
3.1.1	Permissible combinations of internal wiring/external cable sizes for overcurrent and short circuit protection.		Pass
3.1.1	All interconnecting cables protected against overcurrent and short circuit.		Pass
3.2	Wiring methods permit connection of equipment to primary power supply in accordance with the NEC and CEC, Part 1.		Pass
3.2.1	Permitted use for flexible cords and plugs.		Pass
3.2.1	Flexible cords provided with attachment plug rated 125% of equipment current rating.		N/A
3.2.1	Any Class II equipment provided with 15 or 20 A standard supply outlets, Edison-base lampholders or single pole disconnect device provided with a polarized type attachment plug.	Equipment is not Class II.	N/A
3.2.1.2	Equipment intended for connection to DC mains supply power systems complies with special wiring requirements (e.g., no permanent connection to supply by flexible cord).	Equipment is not intended for DC mains supply	N/A
3.2.1.2	Equipment with one pole of the DC mains supply connected to both the equipment mains input terminal and the main protective earthing terminal provided with special instructions and construction provisions for earthing		N/A
3.2.1.2	Equipment with means for connecting supply to earthing electrode conductor has no switches or protective devices between supply connection and earthing electrode connection.		N/A
3.2.1.2	Special markings and instructions for equipment with provisions to connect earthed conductor of a DC supply circuit to earthing conductor at the equipment.		N/A
3.2.1.2	Special markings and instructions for equipment with earthed conductor of a DC supply circuit connected to the earthing conductor at the equipment.		N/A
3.2.1.2	Terminals and leads provided for permanent connection of DC powered equipment to supply marked to indicate polarity if reverse polarity may result in a hazard.		N/A
3.2.3	Permanently connected equipment has provision for connecting and securing a field wiring system	Equipment is not permanently connected.	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	(i.e. conduit, or leads etc.) per the NEC and CEC, Part 1.		
3.2.3	Permanently connected equipment may have terminals or leads not smaller than No. 18 AWG (0.82 mm²) and not less than 152 mm in length for connection of field installed wiring.		N/A
3.2.3	If supply wires exceed 60 °C, marking indicates use of 75 °C or 90 °C wiring for supply connection as appropriate.		Pass
3.2.3	Equipment compatible with suitable trade sizes of conduits and cables.		Pass
3.2.5	Length of power supply cord limited to between 1.5 and 4.5 m unless shorter length used when intended for a special installation.		Pass
3.2.5	Conductors in power supply cords sized according to NEC and CEC, Part I.		Pass
3.2.5	Power supply cords and cord sets incorporate flexible cords suitable for the particular application.		Pass
3.2.6	Strain relief provided for non-detachable interconnecting cables not supplied by a limited power source.		Pass
3.2.9	Adequate wire bending space and volume of field wiring compartment required to properly make the field connections.	Equipment is not permanently connected.	N/A
3.2.9	Equipment intended solely for installation in Restricted Access Locations using low voltage d.c. systems may not need provision for connecting and securing a field wiring system. A method of securing wiring or instructions provided to ensure the wiring is protected from abuse.		N/A
3.3	Field wiring terminals provided for interconnection of units for other then LPS or Class 2 circuits also comply with 3.3.	No field wiring terminals provided.	N/A
3.3	Interconnection of units by LPS or Class 2 conductors may have field wiring connectors other than those specified in 3.3 if wiring is reliably separated.		N/A
3.3.1	Terminals for the connection of neutral conductor identified by a distinctive white marking or other equally effective means.		N/A
3.3.3	Wire binding screw terminal permitted for connection of No. 10 AWG (5.3 mm²) or smaller		N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	conductor if provided with upturned lugs, cupped washer or equivalent retention.		
3.3.4	Terminals accept wire sizes (gauge) used in the U.S. and Canada.		N/A
3.3.4	Terminals accept current-carrying conductors rated 125% of the equipment current rating.		N/A
3.3.6	Field wiring terminals marked to indicate the material(s) of the conductor appropriate for the terminals used.	No field wiring terminals provided.	N/A
3.3.6	Connection of an aluminum conductor not permitted to terminal for equipment earthing conductor.		N/A
3.3.6	Field wiring connections made through the use of suitable pressure connectors (including set screw type), solder lugs or splices to flexible leads.		N/A
3.4.2	Separate motor control device(s) required for cord-connected equipment rated more than 12 A, or with motor rated more than 1/3 hp or more than 120 V.		N/A
3.4.8	Vertically mounted disconnect devices oriented so up position of handle is "on".		N/A
3.4.11	For computer-room applications, equipment with battery systems capable of supplying 750 VA for 5 min require battery disconnect means.	No batteries provided.	N/A
4.2.8.1	Special opening restrictions for enclosures around CRTs with face dimension of 160 mm or more.	No CRTs provided	N/A
4.2.9	Compartment housing high-pressure lamp marked to indicate risk of explosion.	No high pressure lamps provided.	N/A
4.3.2	Loading test for equipment with handle(s) used to support more than 9 kg tested at four times the weight of the unit.	No carrying handles provided.	N/A
4.3.6	In addition to the IEC requirements, Direct Plug-in Equipment complies with UL 1310 or CSA 223 mechanical assembly requirements.	Equipment is not direct plug-in	N/A
4.3.12	The maximum quantity of flammable liquid stored in equipment complies with ANSI/NFPA 30(Table NAE.6).	No flammable liquids.	N/A
4.3.12	Equipment using replenishable liquids marked to indicate type of liquid to be used.	No liquids provided.	N/A
4.3.13.2	Equipment that produces x-radiation and does not comply with 4.3.12 under all conditions of servicing marked to indicate the presence of radiation where	No radiation produced	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	readily visible.		
4.3.13.5	Requirements contained in the applicable national codes and regulations apply to lasers (21 CFR 1040 and REDR C1370).	The product covered by this report employs indicating LEDs the product was not evaluated to IEC 60825-1. See Miscellaneous Enclosure for manufacturer's data sheets showing emission measurements. Additional testing and evaluation may be required based on auditing Agency's discretion.	N/A
4.7	Automated information storage equipment intended to contain more than 0.76 m^3 of combustible media requires provision for automatic sprinklers or a gaseous agent extinguishing system.		N/A
4.7.3.1	Equipment for use in environmental air space other than ducts or plenums provided with metal enclosure or with non-metallic enclosure having adequate fire-resistance and low smoke producing characteristics. Low smoke-producing characteristics evaluated according to UL 2043. Equipment for installation in space used for environmental air as described in Sec. 300-22(c) of the NEC provided with instructions indicating suitability for installation in such locations.	Not intended for use in environmental air space.	N/A
4.7.3.1	Flame spread rating for external surface of combustible material with exposed area greater than 0.93 m^2 or a single dimension greater than 1.8 m; 50 or less for computer room applications or 200 or less for other applications.	None Provided.	N/A
4.7.3.4	Wire marked "VW-1" or "FT-1" considered equivalent.	VW-1, primary wiring is rated 600 V ac with 0.4 mm thick insulation	Pass
5.1.8.2	Special earthing provisions and instructions for equipment with high touch current due to telecommunication network connections.	No TNV circuits.	N/A
5.1.8.3	Touch current due to ringing voltage for equipment containing telecommunication network leads.		N/A
5.3.6	Overloading of SELV connectors and printed wiring board receptacles accessible to the operator.		N/A
5.3.6	Tests interrupted by opening of a component repeated two additional times.		N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
5.3.8.1	Test interrupted by opening of wire or trace subject to certain conditions.	Equipment is not direct plug-in.	N/A
6	Specialized instructions provided for telephones that may be connected to a telecommunications network.		N/A
6	Marking identifying function of telecommunication type connectors not used for connection to a telecommunication network.		N/A
6.2.1	Special requirements for enameled wiring used as electrical separation provided between parts connected to telecommunication network and telecommunication circuitry intentionally isolated from network.	No TNV circuits.	N/A
6.2.1	Digital line termination equipment (e.g., NCTE) subject to separation requirements.	No TNV circuits.	N/A
6.3	Equipment remotely powered over telecommunication wiring systems provided with specialized markings adjacent to the connection.	None provided.	N/A
6.3	Overcurrent protection incorporated into equipment to provide power over telecommunication wiring system not interchangeable with devices of higher ratings if operator replaceable.		N/A
6.4	Additional requirements for equipment intended for connection to a telecommunication network using cable subject to overvoltage from power line failures (Fig. 6C).	No TNV circuits.	N/A
6.4	Where 26 AWG line cord required by Fig. 6C, either the cord is provided with the equipment or described in the safety instructions.		N/A
6.5	Acoustic pressure from an ear piece less than 136 dBA for short duration disturbances, and less than 125 dBA for handsets, 118 dBA for headsets, and 121 dBA for insert earphones, for long duration disturbances.		N/A
7	Equipment associated with the cable distribution system may need to be subjected to applicable parts of Chapter 8 of the NEC.	No connections to cable distribution systems.	N/A
H	Ionizing radiation measurements made under single fault conditions in accordance with the requirements of the Code of Federal Regulations 21 CFR 1020 and the Canadian Radiation Emitting Devices Act, REDR C1370.	Equipment dose not generate ionizing radiation	N/A
M.2	Continuous ringing signals evaluated to Method A	No ringing signals.	N/A

IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
	subjected to special accessibility considerations.		
M.4	Special requirements for message waiting and similar telecommunications signals.		N/A
NAC	Equipment intended for use with a generic secondary protector marked with suitable instructions.	No TNV circuits.	N/A
NAC	Equipment intended for use with a specific primary or secondary protector marked with suitable instructions.		N/A
NAF	Household/Home Office Document Shredders		N/A
NAF.1.7	Markings and instructions alert the user to key safety considerations related to use of shredders, including not intended to be used by children, avoid touching document feed opening, avoid clothes and hair entanglement, and avoid aerosol products.	Equipment is not a shredder.	N/A
NAF.2.8.3	Safety interlock cannot be inadvertently activated by the articulated accessibility probe (figure NAF.1).		N/A
NAF.3.4	Provided with an isolating switch complying with 3.4.2, including 3 mm contact gap, with appropriate markings associated with the switch.		N/A
NAF.4.4	Hazardous moving parts are not accessible to the user, as determined using the articulated accessibility probe (figure NAF.1) and the accessibility probe/wedge (figures NAF.2/NAF.3).		N/A

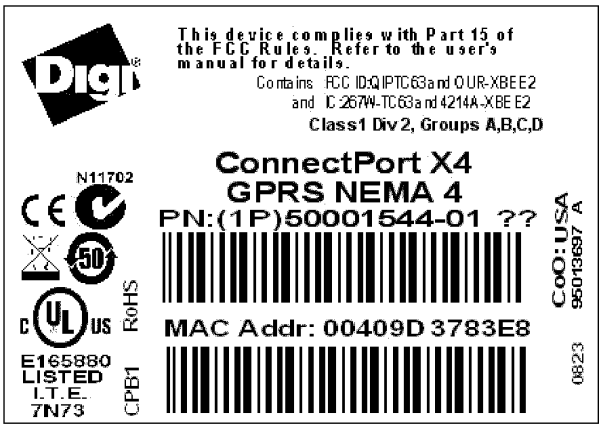
IEC 60950-1			
SubClause	Difference + Test	Result - Remark	Verdict
United Kingdom - Differences to IEC 60950-1:2001, First Edition			
2.6.3.3	The current rating of the circuit shall be taken as 13 A, not 16 A.		N/A
2.7.1	To protect against excessive currents and short-circuits in the primary circuit of direct plug-in equipment, protective device shall be included as integral parts of the direct plug-in equipment.	Equipment is not direct plug-in.	N/A
3.2.1.1	Apparatus which is fitted with a flexible cable or cord and is designed to be connected to a mains socket conforming to BS 1363 by means of that flexible cable or cord and plug, shall be fitted with a "standard plug" in accordance with Statutory Instrument 1786: 1994 - The Plugs and Sockets etc. (Safety) Regulations 1994, unless exempted by those regulations. NOTE: "Standard plug" is defined in SI 1786: 1994 and essentially means an approved plug conforming to BS 1363 or an approved conversion plug.	See Enclosure Miscellaneous for Manufacturer's Letter of Assurance. Manufacturer assumes responsibility of providing a cord and plug that is suitable for the country in which it is installed.	N/A
3.2.5.1	A power supply cord with conductor of 1.25 mm² is allowed for equipment with a rated current over 10A and up to and including 13A.	See Enclosure Miscellaneous for Manufacturer's Letter of Assurance. Manufacturer assumes responsibility of providing a cord and plug that is suitable for the country in which it is installed.	N/A
3.3.4	The range of conductor sizes of flexible cords to be accepted by terminals for equipment with a rated current of over 10 A up to and including 13 A is 1.25 mm² to 1.5 mm² nominal cross-sectional area.	Equipment not rated over 10A	Pass
4.3.6	The torque test is performed using a socket outlet complying with BS 1363 and the plug part of Direct Plug-In Equipment shall be assessed to BS 1363: Part 1, 12.1, 12.2, 12.3, 12.9, 12.11, 12.12, 12.16 and 12.17, except that the test of 12.17 is performed at not less than 125 °C.	Equipment is not direct plug-in.	N/A

Enclosure

Marking Plate

Supplement Id	Description
13-01	Name Plate
13-02	Voltage Rating marking plate

MarkingPlate ID 13-01



2.5" x 1.75"

FILL IN THE REQUIRED LABEL INFORMATION:

ENGINEERING

1) Text Label Part Number: 95013697 , 2) Text Label Revision: A ,

Used on Label Part Number (when applicable, 94million): N/A .

3) Digi Part Number: 50001544-01 , w/MAC

&

MARKETING

4) Description #1 (18 Characters): ConnectPort X4 ,

5) Description #2 (18 Characters): GPRS NEMA 4 ,
(Use this block for a single line of text)

6) Additional Regulatory Information: Digi Logo; CE; ULcus, LISTED, ITE, 7N73, E165880, ULname:CPB1; FCC Part 15 This device complies with Part 15 of the FCC Rules. Refer to the user's manual for details; WEEE; RoHS; CoO: USA; China50 RoHS; C-Tick N11702 .

Contains FCC ID: QIPTC63 and OUR-XBEE2
and IC: 267W-TC63 and 421A-XBEE2
Class1 Div 2, Groups A,B,C,D UL Name: CPB1 .

Label Stock Digi Part Number: 28000223 .

** When Completed, Place A "PRINTED" Label Over The Diagram **

A	xxxxxxxx	New Release	GO 06/13/08			
REV	ECO/NPRO	DESCRIPTION OF CHANGE	BY:	CKD:	APPR:	DATE:

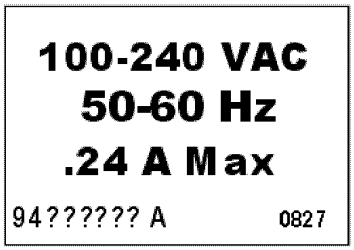
	TITLE: TEXT,2.5" PNBC 50001544-01 LBL	
		DRAWING NO. - REV

Refer to STD OP Proc: 840 2.5" Certification Label Template - Revision A, 09/25/98 Printed: 06/30/2008
95_13697a.doc

MarkingPlate ID 13-01

	DIGI INTERNATIONAL	95013697 A

MarkingPlate ID 13-02

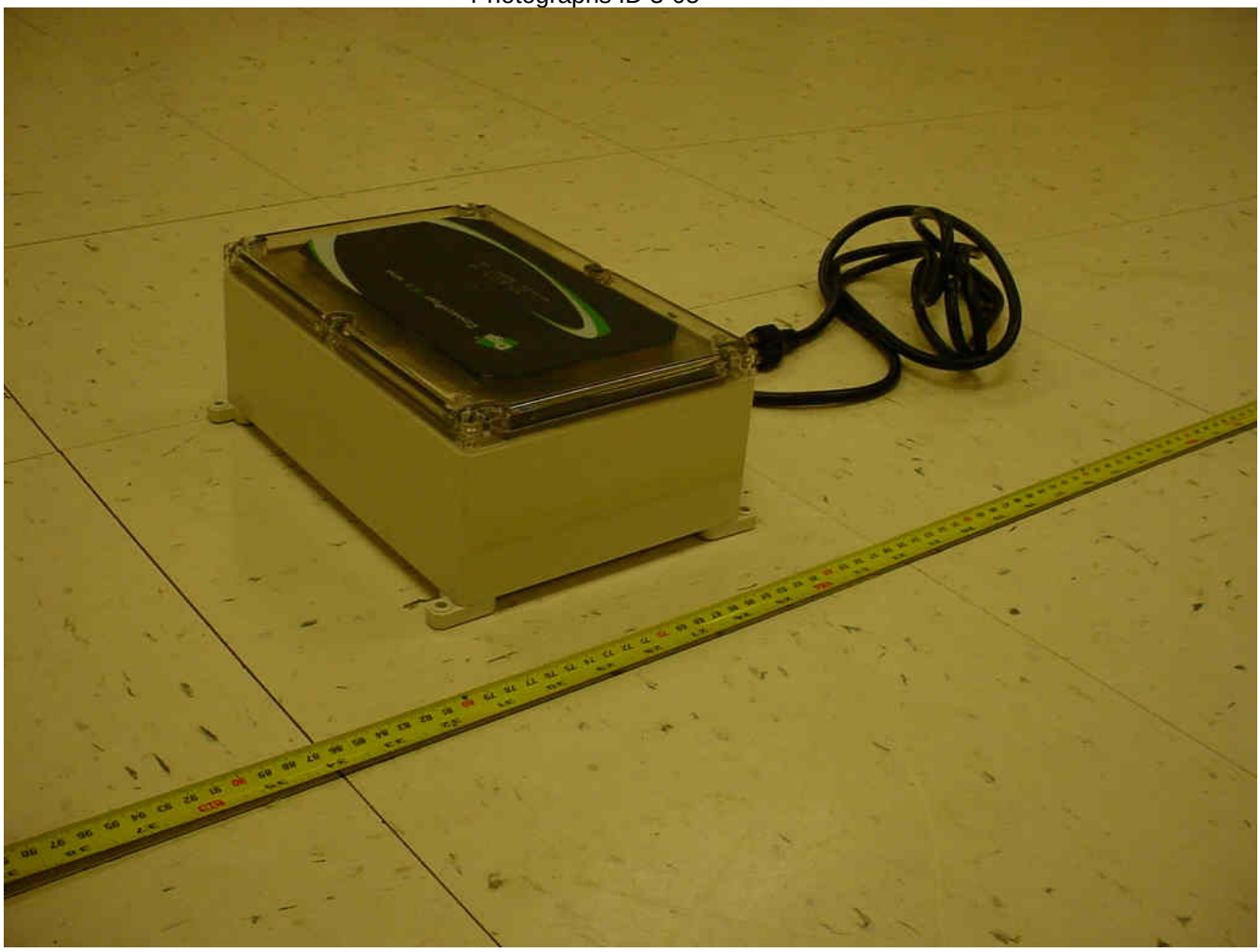


Enclosure

Photographs

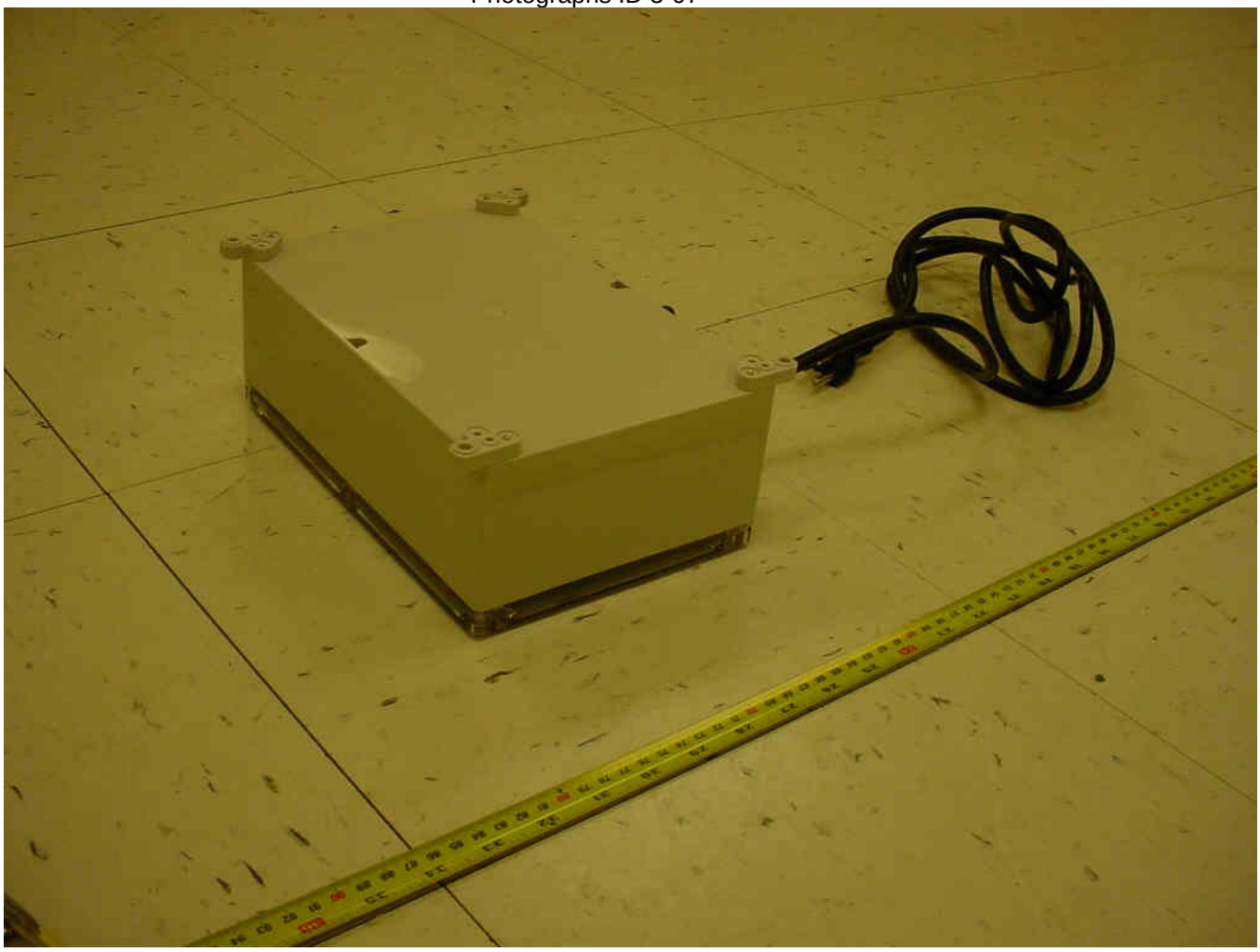
Supplement Id	Description
3-05	Back enclosure
3-06	Front enclosure
3-07	Bottom enclosure
3-08	Internal components
3-09	Internal components Top View
3-10	Power supply

Photographs ID 3-05

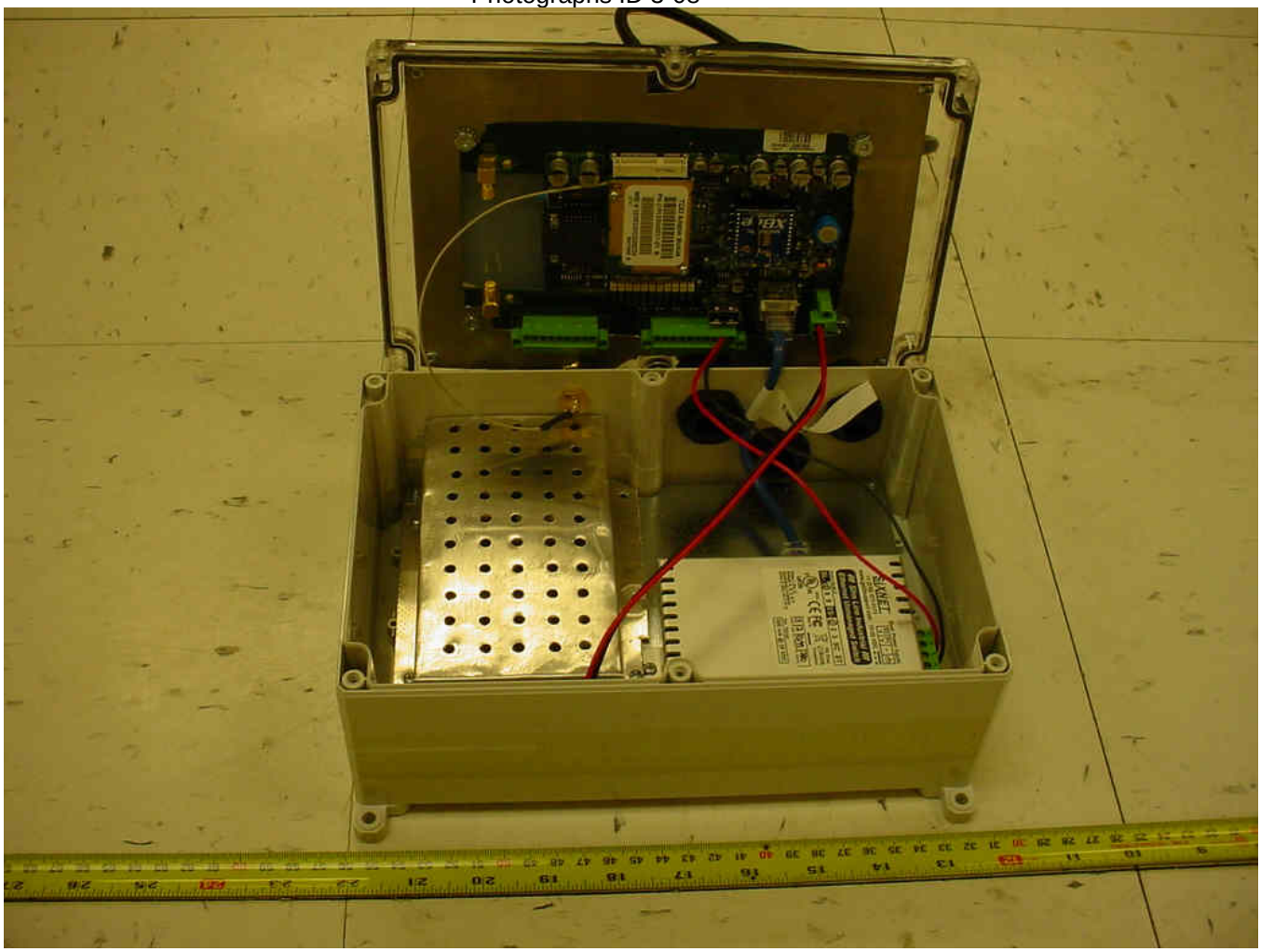


Photographs ID 3-06

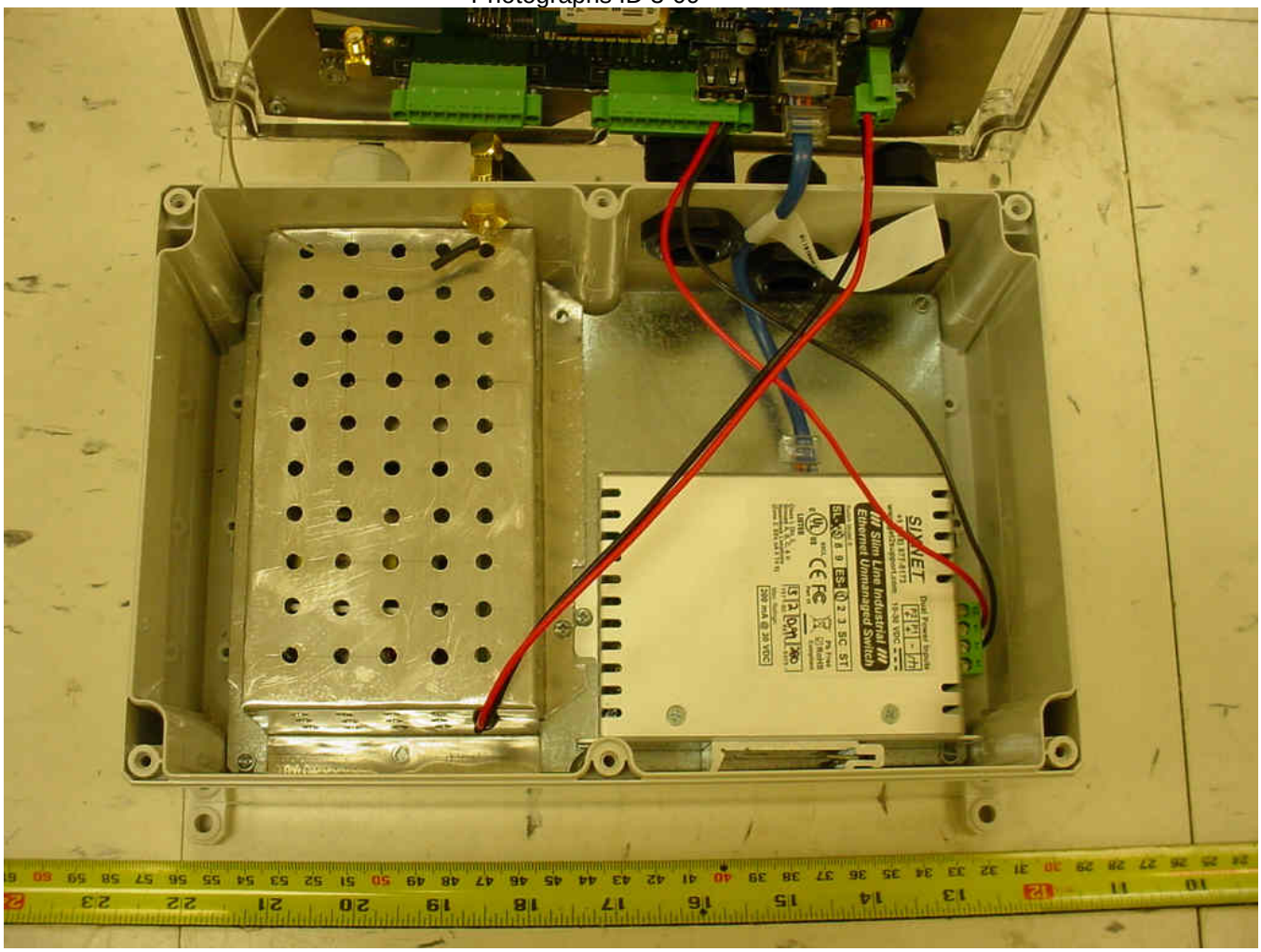
Photographs ID 3-07



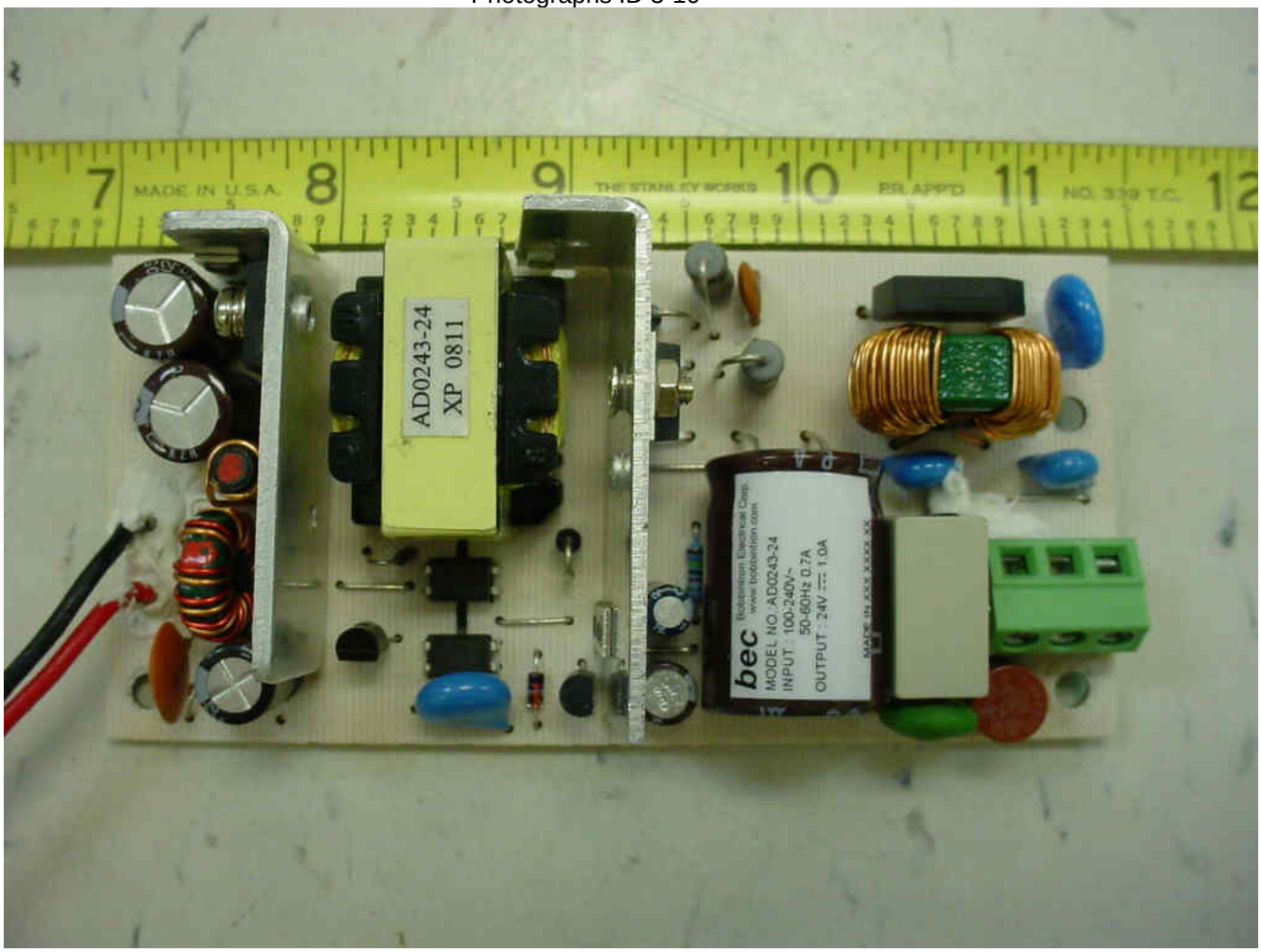
Photographs ID 3-08



Photographs ID 3-09



Photographs ID 3-10



Enclosure

Manuals

Supplement Id	Description
6-01	ConnectPort Manual

Manuals ID 6-01

ConnectPort™ X Family User's Guide

ConnectPort™ X Family Products:
ConnectPort X2, ConnectPort X2 XTend™/XStream® variants
ConnectPort X4, ConnectPort X4 NEMA
ConnectPort X8

90000832_B - PRELIMINARY

Manuals ID 6-01

Manuals ID 6-01

Contents

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

About this guide

Purpose

This guide describes and shows how to provision, configure, monitor, and administer Digi devices.

Audience

This guide is intended for those responsible for setting up Digi devices. 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 devices. It does not cover hardware details beyond a certain level, application development, or customization of Digi devices.

Manuals ID 6-01

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 devices:

- Online help and tutorials in the web interface for the Digi device
- Quick Start Guides
- RealPort® Installation Guide
- Cellular 101 Tutorial
- Digi Connect Family Customization and Integration Guide
- Connectware Manager Getting Started Guide and Operator's Guide
- Release Notes
- Cabling Guides

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

Manuals ID 6-01

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 Digi devices and their product families, types of connections and data paths in which Digi devices can be used, and the interface options available for configuring, monitoring, and administering Digi devices.

Manuals ID 6-01

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.
- For ConnectPort X4 NEMA only: the plug serves as a disconnect device, and must be easily accessible after the device is installed.

Manuals ID 6-01

ConnectPort X Family products

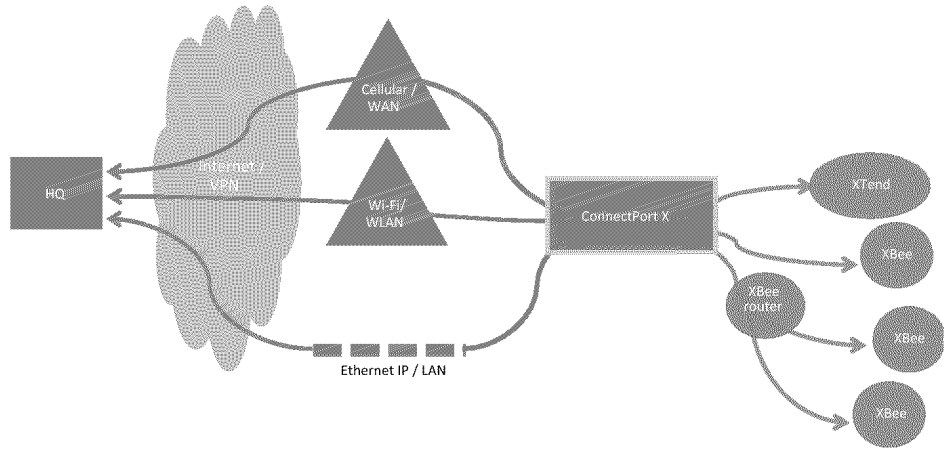
The ConnectPort X Family of products is intended to provide gateway functionality between various network technologies such as Ethernet, cellular, Wi-Fi, and mesh (IEEE 802.15.4 and ZigBee). In addition to providing IP network connectivity between cellular, Wi-Fi and Ethernet networks and devices; ConnectPort X Family products are designed to provide remote connectivity to Mesh networks as well as other devices connected to local ports: USB, 1-Wire, RabbitNet, and asynchronous serial. ConnectPort X Family products act as a coordinator for a mesh network. As with the Connect and Cellular product families, ConnectPort X Family products are supported by Digi's Connectware Manager device management software application, which can be used to remotely manage gateway devices and mesh networks.

Key features of ConnectPort X Family include:

- Network flexibility: gateway functionality for a variety of networks
- MaxStream XBeePro Radio
- Currently Freescale-based, primarily 802.15.4
- Ember-250/ZigBee-based
- Commercial/Industrial Grade
- Connectware Enterprise Management: High-level and detailed views of mesh networks and nodes
- Personal Area Network (PAN) connectivity and management
- Support of Python programming language, for creating a variety of embedded programs and applications
- Remote help desk support through a WatchPort® Camera connection to a USB host port
- Security

Drop-in Networking definitions

This guide uses several terms to describe the networks, connectivity, and data communications involved when a ConnectPort X device is used for Drop-in Networking. The figure shows a ConnectPort X device and its role in Drop-in Networking connectivity.



- *Network* connectivity
- High throughput
- Shared among device networks
- Network types:
  - Cellular / WAN
  - Wi-Fi / WLAN
  - Ethernet IP / LAN

- *Device* connectivity
- Low throughput
- Exclusive to device network
- Network types:
  - 802.15.4
  - ZNet 2.5
  - ZB
  - XSC
  - XTend™
  - XStream®
  - Wi-Fi

Drop-in Networking: Involves *end-to-end device-to-network connectivity*, commonly through gateways, routers, adapters, and embedded modules.

Backhaul network: Involves *network connectivity*, commonly through LAN (Ethernet), WLAN (Wi-Fi), or WAN (cellular).

WPAN (Wireless Personal Area Network): Involves *end device connectivity*, commonly through ZigBee, 802.15.4, and many other public or proprietary technologies.

Features

This is an overview of key features in Digi devices. 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 devices, including:

- The Digi Device Setup Wizard, a wizard-based tool for assigning an IP address to a Digi device, minimally configuring it, and installing RealPort software on a PC or server.
- A web-based interface for configuring, monitoring, and administering Digi devices.

  For Digi devices that ship with a default IP address, simply connecting a laptop computer to the Ethernet port of these products allows direct access to the web interface for configuration.
- A command-line interface.
- Simple Network Management Protocol (SNMP).

Quick reference for configuring features

This guide primarily focuses on configuring, monitoring, and administering Digi devices from the web 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 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 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.	188
■ Python program file management.	**Application > Python**	190
■ Backup/restore a configuration from a TFTP server on the network	**Administration > Backup/Restore**	190
■ Update firmware	**Administration > Update Firmware**	191
■ Reset configuration to factory defaults	**Administration > Factory Default Settings**	192
■ System information, including device identifiers and statistics	**Administration > System Information**	193
■ Reboot the Digi device	**Administration > Reboot**	193
■ Certificate and key management, including X.509, VPN, SSL, SSH	**Administration > X.509 Certificate and Key Management**	189
Alarms	**Configuration > Alarms**	130
Autoconnection: automatically connect a user to a server or network device	**Configuration > Serial Ports > *port* > Profile Settings > TCP Sockets > Automatically establish TCP connections**	120
Camera settings for ConnectPort X Family products	**Configuration > Camera**	128
Connection management:		

Manuals ID 6-01

Feature/task	Path to feature in the web interface	See page
■ Manage serial port connections	**Management > Serial Ports**	166
■ Manage Virtual Private Network (VPN) connections	**Management > Connections > Virtual Private Network (VPN) Settings**	166
■ Manage active system connections	**Management > Connections > Active System Connections**	166
■ Manage network services	**Management > Network Services** (Currently only DHCP server settings managed from here)	167
Domain Name System (DNS):		
■ DNS Client	**Configuration > Network > IP Settings > Primary DNS** and **Secondary DNS**	65
■ Dynamic DNS (DDNS) update	**Configuration > Network > Dynamic DNS Update Settings**	72
Dynamic Host Configuration Protocol (DHCP) server	To configure a DHCP server: **Configuration > Network > DHCP Server Settings** To start and stop and show status of a DHCP server: **Management > Network Services > DHCP Server Management**	65
Ethernet settings	**Configuration > Network > Advanced Network Settings**	101
Event logging for the Digi device	**Management > Event Logging**	167
Help on configuring features	**Help** button on each page.	
Host name for a device	**Configuration > Network > Advanced Network Settings > Host Name**	101
Industrial Automation (IA)	**Configuration > Serial Ports > Select Port Profile > Industrial Automation** The Industrial Automation port profile should address most configuration scenarios. To fine-tune your IA settings, use the "set ia" command from the command line. See the **set ia** command description in the *Digi Connect Family Command Reference*. For additional information on configuring Industrial Automation, see this web site: http://www.digi.com/support/ia	143
IP address settings:		
■ Using static IP addresses	**Configuration > Network > IP Settings**	54, 65
■ Using DHCP	**Configuration > Network > IP Settings** and **Configuration > Network > DHCP Server Settings**	55, 65,
■ Using Auto IP	**Configuration > Network > Advanced Settings**	55, 101

Manuals ID 6-01

Feature/task	Path to feature in the web interface	See page
IP filtering / access control	**Configuration > Network > IP Filtering Settings**	74
IP forwarding: Network Address Translation (NAT) and port forwarding configuration/static routes	**Configuration > Network > IP Forwarding Settings**	75
IP pass-through	**Configuration > Network > IP Pass-through**	77
Mesh network configuration and management:		
■ Mesh network configuration through web UI	**Configuration >** mesh **Network**	112
■ Mesh network configuration through Connectware Manager	**Mesh Networks and Mesh Node Properties** views	150
■ Mesh network monitoring/ management through web UI	**Administration > System Information >** mesh **Network** See also Connectware Manager's **Mesh Network** view and detailed view of network nodes	170
■ Mesh network monitoring/ management through command line	**set mesh** **display mesh** **info zigbee_sockets**	184
Mobile (cellular) settings:		
■ Provisioning CDMA cellular modules	**Configuration > Mobile** For Digi Cellular product that have a CDMA cellular module, provisioning must be performed once. To launch a wizard for provisioning the module, go to **Configuration > Mobile**. Under Mobile Service Provider Settings, click the **Provision Device** button. Provisioning can also be performed from the command line: ■ To provision the CDMA module: **provision** ■ To display existing provisioning parameters: **display provisioning**	104
■ Mobile service provider and connection settings	**Configuration > Mobile** Settings displayed vary by mobile service provider.	102, 108
■ SureLink™ Settings	**Configuration > Mobile > SureLink Settings**.	108
Modem emulation	**Configuration > Serial Ports > Port Profile Settings > Modem Emulation** See the *Connect Family Command Reference* for modem emulation commands.	122
Port profiles: sets of preconfigured serial-port settings for a particular connection and use scenario	**Configuration > Serial Ports > Port Profile Settings**	119

Manuals ID 6-01

Feature/task	Path to feature in the web interface	See page
Python program file management: loading and running custom programs authored in the Python programming language.	**Application > Python** For more information on writing and running Python programs, see the *Digi Python Programmer's Guide*.	190
RealPort (COM port redirection) configuration	**Configuration > Serial Ports > *port* > Port Profile Settings > RealPort** See also the *RealPort Installation Guide*.	120
Remote device management through Connectware Manager	**Configuration > Remote Management**	135
Reverting configuration settings	**Administration > Factory Default Settings**	192
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**	119
■ Secure Shell Server (SSH)	**Configuration > Security > Enable SSH public key authentication** **Network > Network Services > Enable Secure Shell Server (SSH)**	142, 70
■ Establish/change user name for a user	**Configuration > Security**	140
■ Issue a new/changed password to a user	**Configuration > Security**	
Serial port configuration:		
■ Basic serial port settings	**Configuration > Serial Ports > Basic Serial Settings**	124
■ Advanced serial port settings	**Configuration > Serial Ports > Advanced Serial Settings**	124
■ Port profiles: associate a serial port with a set of preconfigured port settings for a specific use	**Configuration > Serial Ports > Port Profile Settings**	119
■ RCI over serial mode	**Configuration > Serial Ports > Advanced Serial Settings**	124
■ RTS Toggle	**Configuration > Serial Ports > Advanced Serial Settings**	124
■ TCP serial connections	**Configuration > Serial Ports > *port* > Port Profile Settings > TCP Sockets port profile**	120
■ UDP serial characteristics	**Configuration > Serial Ports > *port* > Port Profile Settings > UDP Sockets port profile**	121
Simple Network Management Protocol (SNMP):		

Manuals ID 6-01

Feature/task	Path to feature in the web interface	See page
■ Configure SNMP through the web interface	**Configuration > System > Simple Network Management Protocol (SNMP) Settings**	134
■ Enable/disable SNMP service	**Configuration > Network > Network Services**	69
■ Enable/disable SNMP alarm traps	**Configuration > Alarms > *alarm* > Send SNMP trap to following destination when alarm occurs**	132, 133
■ 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 interface, on the pages listed above.	149
System information: assign system-identifying information to a device	**Configuration > System > Device Identity Settings**	134
Socket Tunnel Settings	**Configuration > Network > Socket Tunnel Settings**	76
Statistics for Digi devices	**Administration > System Information**	156
Status of Digi devices	**Management > Serial Ports, Connections, Network Services**	166
VPN (Virtual Private Network)	To configure VPN: **Configuration > Network > Virtual Private Network (VPN) Settings** To manage VPN: **Management > Connections > Virtual Private Network (VPN) Connections**	

Hardware features

A summary of hardware features, including power-supply information, is in "Hardware specifications" on page 196.

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 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 69. 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 Digi devices include a Robust on-board TCP/IP stack with a built-in web server. Supported protocols 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 27 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)
- Point to Point Protocol (PPP)
- Secure Shell (SSHv2)
- Generic Routing Encapsulation (GRE) Passthrough
- Encapsulating Security Payload (ESP)
- ESP Passthrough

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

Manuals ID 6-01

Serial data communication over TCP and UDP

Digi devices support 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, an extension of the Telnet protocol
- 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 alternatives" on page 33.

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 alternatives" on page 33.

Manuals ID 6-01

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 devices support SNMP Version 1. For more information on SNMP as a device-management interface, see "Simple Network Management Protocol (SNMP)" on page 48.

Supported RFCs and MIBs

Digi devices 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 displaying device information.
- 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 devices. For more information, see "Security features" on page 35.

Telnet

Digi devices 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 in Digi devices" on page 37. 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 devices 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. Digi Cellular and ConnectPort X devices support PPP as the connection protocol from the Digi Cellular device to the cellular IP network with NAT (Network Address Technology).

Network Address Translation (NAT)/Port Forwarding

Network Address Translation (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.

Generic Routing Encapsulation (GRE) Passthrough
Encapsulating Security Payload (ESP)
ESP Passthrough

Generic Routing Encapsulation (GRE) and Encapsulating Security Payload (ESP) are routing protocols that are used to route (tunnel) various types of information between networks.

GRE applies to the encapsulation of IP datagrams tunnelled through the internet. The encapsulation includes security, typically in the form of IPSec (IP security), and is most commonly found in VPN (Virtual Private Network) implementation. RFC (Request For Comment) 1701 and 1702 define these standards.Similarly, ESP is used in conjunction with IPsec as a possible way of carrying IP packets for a Virtual Private Network (VPN) setup. ESP is defined in RFC 2406.

In ESP Passthrough and GRE Passthrough, inbound IPsec ESP or GSP protocol traffic is forwarded from to a VPN device connected to the Digi device's Ethernet port.

Note: If an Auto-key Internet Key Exchange (IKE)-based VPN is used, UDP port 500 must also be forwarded.

Mobile/Cellular features and protocol support

Provisioning wizard

For Digi devices equipped with a Code-Division Multiple Access (CDMA)-based cellular modem, a wizard is available in the web interface to properly configure the Digi device with the required configuration used to access the mobile network. The wizard allows for both automatic and manual provisioning for a variety of mobile service providers.

Digi SureLink™

Digi Cellular Family and ConnectPort X Family products support the Digi SureLink™ feature. Digi SureLink provides an "always-on" mobile network connection to ensure that a Digi device is in a state where it can connect to the network. It does this through hardware reset thresholds and periodic tests of the connection.

Manuals ID 6-01

Mobile/Cellular protocols

Mobile/cellular protocols supported in ConnectPort X Family products include, unless otherwise noted:

- Global System for Mobile communication (GSM)
- Code-Division Multiple Access (CDMA)
- General Packet Radio Service (GPRS)
- Enhanced Data Rates for GSM Evolution (EDGE)
- Universal Mobile Telecommunications Service (UMTS)
- Evolution-Data Optimized (EV-DO, EVDO, or 1xEV-DO)

Global System for Mobile communication (GSM)

The GSM protocol is a digital mobile telephone system used in Europe and other parts of the world. There are three major types of digital mobile systems and GSM is the most widely used. GSM compresses and digitizes data and sends it down a channel along with two other streams of user data - each in its own time slot.

Code-Division Multiple Access (CDMA)

CDMA is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHZ bands and through an analog-to digital conversion enhances privacy and makes cloning difficult.

General Packet Radio Service (GPRS)

GPRS is based on Global System for Mobile (GSM) communication. GPRS is a packet-based wireless communication service that transports data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. Higher data rates allow users more flexibility in the media they transmit. In theory, GPRS packet-based service costs users less than circuit-switched services since communication channels are being used on a shared-use, as-packets-are-needed basis rather than dedicated only to one user at a time. It should also be easier to make applications available to mobile users because the faster data rate means that middleware currently needed to adapt applications to the slower speed of wireless systems will no longer be needed.

Enhanced Data Rates for GSM Evolution (EDGE)

EDGE is a faster version of the GSM wireless service and designed to deliver data at rates up to 384 Kbps and enable the delivery of multimedia and other broadband applications to mobile phone and computer users. The EDGE standard is built on the existing GSM standard, using the same time-division multiple access frame structure and existing cell arrangements.

Universal Mobile Telecommunications Service (UMTS)

UMTS is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps) that offers a consistent set of services to mobile computer and phone users no matter where they are located in the world.

Manuals ID 6-01

Based on the Global System for Mobile (GSM) communication standard, UMTS, endorsed by major standards bodies and manufacturers, is the planned standard for mobile users around the world and is at present still being made available. Once UMTS is fully available geographically, computer and phone users can be constantly attached to the Internet as they travel and, as they roam, have the same set of capabilities no matter where they travel to. Users will have access through a combination of terrestrial wireless and satellite transmissions. Until UMTS is fully implemented, users can have multi-mode devices that switch to the currently available technology (such as GSM 900 and 1800) where UMTS is not yet available.

Today's cellular telephone systems are mainly circuit-switched, with connections always dependent on circuit availability. A packet-switched connection, using the Internet Protocol (IP), means that a virtual connection is always available to any other end point in the network. It will also make it possible to provide new services, such as alternative billing methods (pay-per-bit, pay-per-session, flat rate, asymmetric bandwidth, and others). The higher bandwidth of UMTS also promises new services, such as video conferencing. UMTS promises to realize the Virtual Home Environment (VHE) in which a roaming user can have the same services to which the user is accustomed when at home or in the office, through a combination of transparent terrestrial and satellite connections.

The electromagnetic radiation spectrum for UMTS has been identified as frequency bands 1885-2025 MHz for future IMT-2000 systems, and 1980-2010 MHz and 2170-2200 MHz for the satellite portion of UMTS systems.

Evolution-Data Optimized (EV-DO, EVDO, or 1xEV-DO)

EVDO is a wireless radio broadband data standard adopted by many CDMA mobile phone service providers. It is standardized by 3GPP2, as part of the CDMA2000 family of standards. Compared to 1xRTT (CDMA2000 1x) networks, or GPRS and EDGE networks, 1xEV-DO is significantly faster.

IP address assignment alternatives

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

- Static IP: Assign a specific IP address to a device, through the Digi Device Setup Wizard, the web 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 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 54.

RealPort software

Digi devices use the patented RealPort COM/TTY port redirection for Microsoft Windows. 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 devices also support 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.

Manuals ID 6-01

Alarms

Digi devices can be configured to issue alarms, in the form of email message or SNMP traps, when certain device events occur. These events include certain data patterns being detected in the data stream, and cellular alarms for signal strength and amount of cellular traffic for a given period of time. 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. Alarms can also be forwarded to Connectware Manager for display and management in that platform. For more information on configuring alarms, see "Configure alarms" on page 130.

Modem emulation

Digi devices 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 and Cellular 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 devices are documented in the *Digi Connect Family Command Reference*.

Security features

Security-related features in Digi devices 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, 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.
- Encryption:
  - 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 device.
- 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 device 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 devices 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 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 on the Digi Connect Integration Kit customization tools and resources and for assistance with customization efforts.

Supported connections and data paths in Digi devices

Digi devices 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.

This discussion of connections and data paths may be helpful in understanding 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

- 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

- 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 devices 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

- 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 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

This is an overview of the configuration capabilities and interfaces for Digi devices; Chapter 2, "Configure Digi devices" covers them 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.
- Mobile (cellular) configuration: Specifying the mobile service provider and mobile connection settings for the device.
- Serial port configuration: Specifying the serial port characteristics for the device.
- 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 devices, 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 interface for the devices.
- A web-based interface embedded with the product, providing device configuration profiles for quick serial-port configuration and other settings.

  For Digi Cellular Family products, the web interface is the preferred interface for configuration. As all ConnectPort X Family products ship with a default static IP address of **192.168.1.1** for the Ethernet port. Simply connecting a laptop computer to the Ethernet port allows direct access to the web interface for configuration.
- 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.
- Simple Network Management Protocol (SNMP).

Manuals ID 6-01

The Digi Device Setup wizard

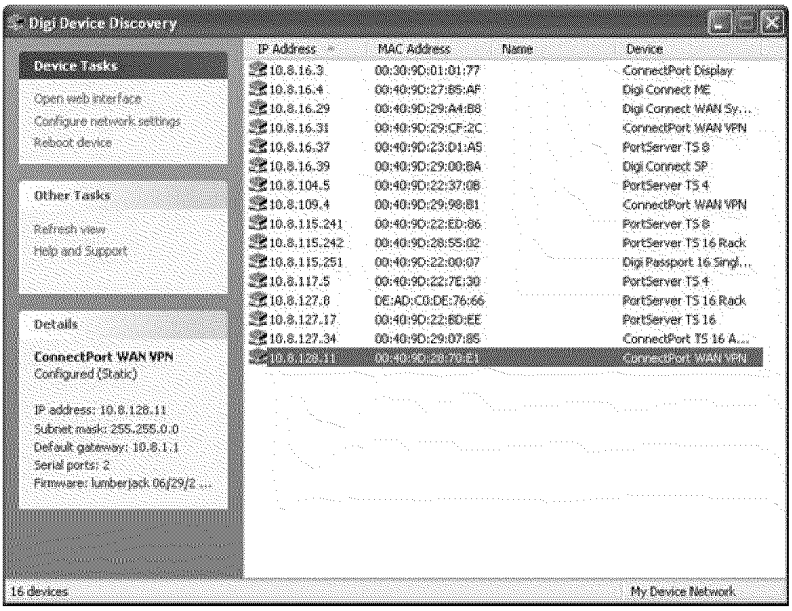
The Digi Device Setup Wizard is a wizard for quick initial configuration of Digi devices. It is provided on the CD shipped with each product. It assigns an IP address for the device, configures the device's serial port parameters based on a selected configuration scenario called a port profile, and determines whether RealPort software needs to be installed.

Digi Cellular FamilyConnectPort X Family products have a predefined IP address of **192.168.1.1** for the Ethernet port (see "Default IP address" on page 54). Instead of using the Digi Device Setup Wizard to obtain an IP address for the Ethernet port, you can simply connect to the Ethernet port of the Digi device, and directly access the web interface for device configuration. For these products, consider the Digi Device Setup Wizard as an alternative method for obtaining an IP address.

Manuals ID 6-01

Digi Device Discovery utility

The Digi Device Discovery utility locates Digi devices on a network and allows for opening the web interface for discovered devices, configuring network setttings, and rebooting the device. It uses a Digi International-proprietary protocol, Advanced Digi Discovery Protocol (ADDP), to discover the Digi devices on a network, and displays the discovered devices in a list, for example:



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 that can send multicast IP packets to a network. It sends out a User Datagram Protocol (UDP) multicast packet to all devices on the network. Devices supporting ADDP reply to this UDP multicast with their configuration information. Even devices that do not yet have an IP address assigned or are misconfigured for the subnet can reply to the UDP multicast packet and be displayed in device discovery results.

Disadvantages include:

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

Manuals ID 6-01

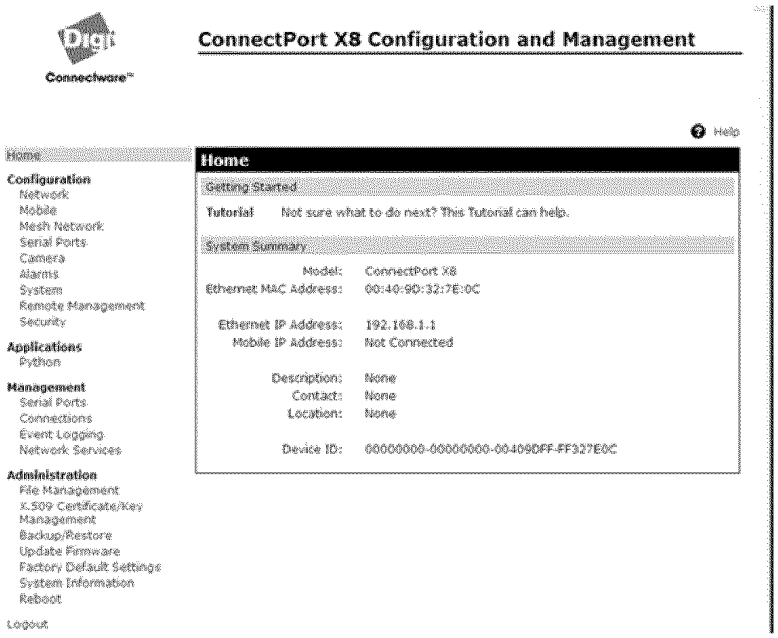
Digi Device Discovery is available on the Digi device's Software and Documentation CD. After installation, it is available from the **Start** menu. Access to the ADDP service can be enabled or disabled, but the network port number for ADDP cannot be changed from its default.

For more information on the Digi Device Discovery utility, see page 58.

The Web interface

A web interface is provided as an easy way to configure and monitor Digi devices. Configurable features are grouped into several categories. These categories vary by product; examples include Network, Serial Port, Alarms, System, Remote Management, Security. 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 interface.



Manuals ID 6-01

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

To access the web interface, enter the Digi 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 interface" on page 57

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

Command-line interface

Digi devices 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 assign the IP address to the Ethernet interface:

```
#> set network ip=192.168.1.1
```

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.

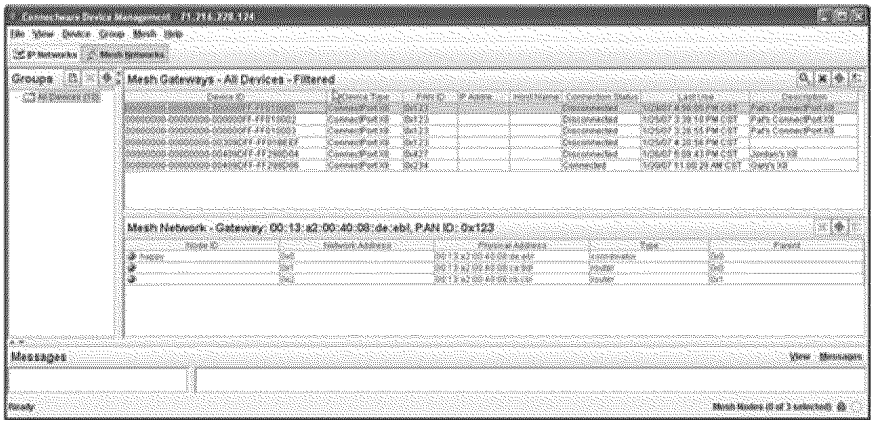
See "Configuration through the command line" on page 146 for more information on this interface. See the *Digi Connect Family Command Reference* for command descriptions and examples of entering configuration commands from the command-line interface. In addition, online help is available for the commands, through the help and '?' commands.

Manuals ID 6-01

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.



Manuals ID 6-01

Advantages of the Connectware Manager interface are:

- Allows multiple devices to be managed (configured and monitored) from one source. This multiple-device, network-view capability is particularly useful for Cellular and ConnectPort X products.
- 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 135. This section shows how to configure Connectware Management settings within Digi devices.
- "Configuration through Connectware Manager" on page 150.
- "Monitoring capabilities from Connectware Manager" on page 183
- *Connectware Manager Getting Started Guide*

Remote Command Interface (RCI)

Remote Command Interface (RCI) is a programmatic interface for configuring and controlling Digi 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 web 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 device to replace the web 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 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 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 devices 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 devices, read/write capabilities are expected to be added to Digi 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 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 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 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 **http://www.rfc-editor.org/rfcsearch.html**, 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 185.

Monitoring capabilities and interfaces

There are several capabilities and interfaces for monitoring Digi devices and managing their connections; these are covered in more detail in Chapter 3, "Monitor and manage Digi devices".

Monitoring Digi devices includes such tasks as checking device status, checking runtime state, viewing serial port operations, and reviewing network statistics, and managing their connections.

Monitoring interfaces

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

- The web interface embedded with the product
- SNMP
- The command-line interface
- Connectware Manager

Web interface

The web interface several screens for monitoring Digi devices:

- Network Status
- Mobile connection 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
  - 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 175.

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.

Connectware Manager is well-suited to managing Cellular and ConnectPort X Family devices and the networks in which the devices reside. Advantages include:

- The ability to view an entire network, and multiple networks, at once
- Easy to view signal strength, link quality, and alarms

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 185.

Administration tasks

Periodically, administrative tasks need to be performed on Digi 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 interface, command line, and Connectware Manager. See Chapter 4, "Administration tasks" for more information and procedures.

Configure Digi devices

CHAPTER 2

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

The primary focus of this chapter is on configuring Digi devices **through the web 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 an IP address using the Digi Device Setup Wizard" on page 54.

Manuals ID 6-01

Default IP address

ConnectPort X Family products ship with a a **default static IP address** for the Ethernet port of **192.168.1.1 and a** a DHCP server enabled by default. Therefore, simply connecting a laptop computer to the Ethernet port of these products allows direct access to the web interface for configuration.

All ConnectPort X Family products have a DHCP server enabled by default. Therefore, simply connecting a laptop computer to the Ethernet port of these products allows direct access to the web interface for configuration.

For details on identifying the IP address that has been assigned through DHCP, see "Configure an IP address using DHCP" on page 55.

Alternate methods for assigning an IP address

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

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

Configure an 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 devices. 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 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 deviceto the network and power it on.
2. Locate the MAC address for the Digi device; it is on a 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 device by its MAC address.
6. Select the Digi device and click **Next**.

7 Follow the instructions in the wizard to assign an IP address for the Digi device. Use the online help supplied with the wizard for information about values and selections on the wizard screens.

Configure an IP address using DHCP

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

All ConnectPort X Family products have a DHCP server enabled by default. Therefore, simply connecting a laptop computer to the Ethernet port of these products allows direct access to the web interface for configuration. The Digi Connect WAN IA ships with the DHCP client enabled, which can then be used to obtain an IP address for your Digi product. For details on identifying the IP address that has been assigned through DHCP, see "Configure an IP address using DHCP" on page 55.

If desired, set up a permanent entry for the Digi device 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 is saved when the device is rebooted. For more information on DHCP server configuration, see "DHCP server settings" on page 65.

Configure an 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 an 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
```

IP addresses and Connectware Manager

The Connectware Manager interface can only change the Ethernet/LAN address for a Digi device. The mobile/cellular device is typically provided by the mobile service provider; check with your mobile service provider on how they handle addresses. To change the IP address, open the web 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 device has 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 device. For example:

   ```
   ping 192.168.2.2
   ```

Configuration through the web interface

Configuring Digi devices through the web interface involves these tasks:

- Change the IP address, as needed. See page 62.
- Open the web interface. See page 57.
- Configure network communications. See page 63.
- Configure mobile (cellular) settings, including provisioning the Digi Cellular Family device, mobile service provider settings, mobile connection settings, and SureLink settings. See page 102.
- Configure Mesh network settings. See page 112.
- Configure the serial ports. See page 119.
- Configure camera settings. See page 128.
- Configure alarms. See page 130.
- Configure security/user features such as user names and password authentication. See page 140.
- Configure system-identifying information and the settings for Simple Network Management Protocol (SNMP). See page 134.
- Configure remote management using a Connectware Manager server. See page 135.
- Configure and run applications available for use. Supported applications vary among Digi devices. See page 142.
  - Configure Industrial Automation/Modbus Bridge. See page 143.
  - Manage programs authored in the Python® programming language. See page 144.

Open the web interface

To open the web interface, either enter the Digi 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 Digi device's IP address 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 device, the Home page of the web interface is displayed. If security has been enabled for the Digi 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 interface is displayed. See "Organization of the web interface" on page 59 for an overview of using the Home page and other linked pages.

   Note The idle timeout automatically logs users out of the web 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 device and open its web interface.

Install Digi Device Discovery utility

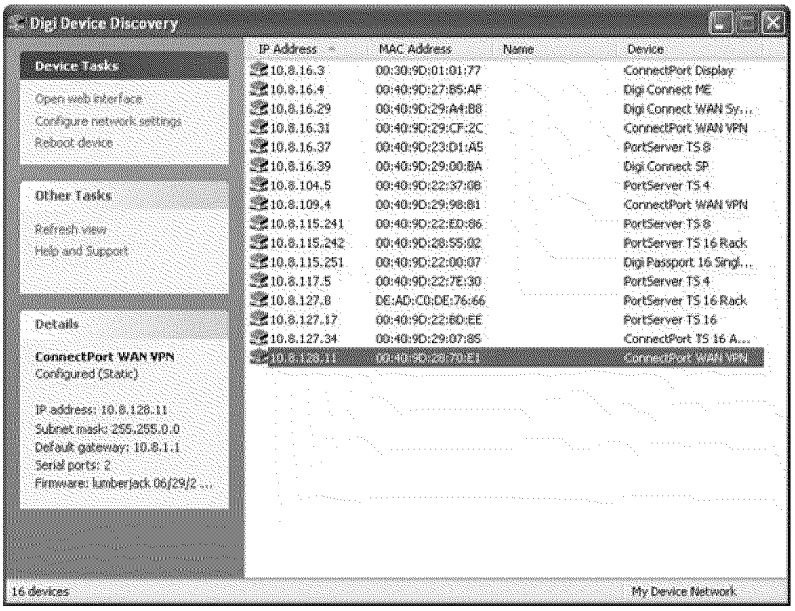
The Digi Device Discovery Utility is available on the Software and Documentation CD. If this utility is not already available on your computer, follow these steps.

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 Digi device from the list and select **Open web interface** in the **Device Tasks** list.



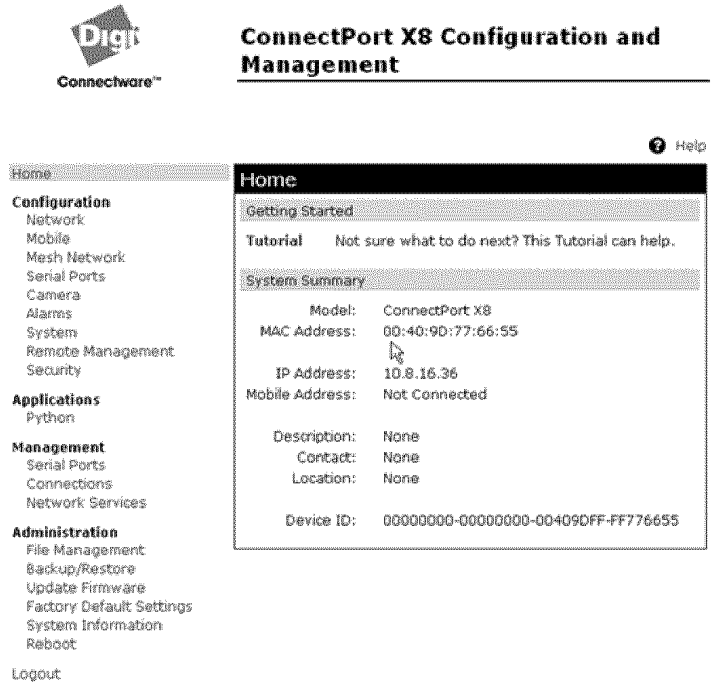
Depending on whether a system administrator has configured password authentication for the device, a login may be required. If a login dialog is displayed, enter the user name and password for the Digi device. The default username is **root** and the default password is **dbps**. If these

defaults do not work, contact the system administrator who initially set up the device. Now configure the Digi device, as described on the following pages.

Organization of the web interface

When web interface is opened, the Home page is displayed.

Here is a home page for a ConnectPort X Family product.



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 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, "Monitor and manage Digi devices".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 device. It does not close the browser window, but displays a logout window. To finish logging out of the web 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.

Manuals ID 6-01

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

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.

Manuals ID 6-01

Application pages

Depending on the Digi device, there may be an **Application** menu item for configuring various applications available for use in the device.

- **Python**: For loading and running custom programs authored in the Python programming language onto ConnectPort X Family devices.

Apply and save changes

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

On each screen, the **Apply** button is used to save any changes to the configuration settings to the Digi 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 Digi 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 192.

Online help

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

Change the IP address from the web interface, as needed

Normally, IP addresses are assigned to Digi devices 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 device's current IP address in the URL address bar.
2. If security is enabled for the Digi 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:

- **Ethernet IP settings:** For viewing IP address settings and changing as needed. See page 65.
- **DHCP Server settings:** For configuring a DHCP server to allow other devices or hosts on this network to be assigned dynamic IP addresses. See page 65.
- **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 69.
- **Dynamic DNS Update settings:** For configuring a Dynamic DNS (DDNS) service that allows a user whose IP address is dynamically assigned to be located by a host or domain name. See page 72.
- **IP Filtering settings:** For configuring the Digi Cellular Family device to only accept connections from specific and known IP addresses or networks. See page 74.
- **IP Forwarding settings:** For configuring the Digi Cellular Family device to forward certain connections to other devices. This is also known as Network Address Translation (NAT) or Port Forwarding. See page 75.
- **Socket Tunnel settings:** For configuring a socket tunnel, used to connect two network devices: one on the Digi Cellular Family device's local network and the other on the remote network. See page 76.
- **Virtual Private Network (VPN) settings:** For configuring Virtual Private Networks, which are used to securely connect two private networks together so that devices may connect from one network to the other network using secure channels. See page 77.
- **IP Pass-through settings:** Configures a Digi Cellular Family device to pass its mobile IP address directly through and to the Ethernet device (router or PC) to which it is connected through the Ethernet port. The Digi Cellular Family device becomes transparent (similar to the behavior of a cable or DSL modem) to provide a bridge from the mobile network directly to the end device attached to the Digi Cellular Family device. See page 77.
- **Virtual Router Redundancy Protocol (VRRP) settings**: For configuring a number of routers to represent a virtual router, which simplifies configuration of hosts on a network.
- **Advanced Network Settings**: Configures the Ethernet Interface speed and mode, TCP/IP settings, TCP keepalive settings, and DHCP settings. See page 101.

Alternatives for configuring network communications

There are three ways a Digi devicecan 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.

Manuals ID 6-01

- **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.

ConnectPort X Family products have two IP addresses: one for Ethernet and one for cellular. All ConnectPort X Family products have a pre-defined default Ethernet Port IP address of 192.168.1.1.

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 deviceby 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 devicecan no longer access the device. In this case, the Digi device must be located the Digi Device Discovery utility, and other network devices that need to communicate with the Digi device must be reconfigured.

Ethernet IP settings

The Ethernet IP Settings page shows how the IP address of the Digi deviceis 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.

DHCP server settings

The DHCP server feature can be enabled in a Digi device to allow other devices or hosts on this network to be assigned dynamic IP addresses. This DHCP server supports a single subnetwork scope.

For the DHCP server to operate, the Digi device must be configured to use a static IP address. For information on how to configure static IP settings, see "Ethernet IP settings" on page 65.

The Digi Connect WAN IA has different factory defaults for DHCP server. The DHCP server is disabled, and DHCP Client enabled.

For information on how to manage the DHCP server, see "Manage DHCP server operation" on page 167.

DHCP terminology

Some key DHCP terms involved in configuring a DHCP server include:

scope

A scope is the full consecutive range of possible IP addresses for a network. A scope typically defines a single physical subnet on your network, to which DHCP services are offered. A scope is the primary way for the DHCP server to manage distribution and assignment of IP addresses and related configuration parameters to its clients on the network.

exclusion range

An exclusion range is a limited sequence of IP addresses within a scope, excluded from DHCP service offerings. Exclusion ranges assure that any addresses in these ranges are not offered by the server to DHCP clients on your network.

address pool

After the scope is defined and exclusion ranges are applied, the remaining addresses form the available address pool within the scope. The addresses in this pool are available for dynamic assignment by the server to DHCP clients on your network.

lease

A lease is the length of time that the DHCP server specifies, during which a client host can use an assigned IP address. When the DHCP server grants a lease to a client, the lease is active. Before the lease expires, the client typically needs to renew its address lease assignment with the DHCP server. A lease becomes inactive when it expires or it is deleted at the server, or if the client actively releases the lease. The duration of a lease determines when it will expire and how often the client needs to renew it with the DHCP server in order to retain the lease.

A DHCP server will never grant a lease to its own address. There is no need for its own address to be in the exclusion range; the DHCP server simply protects its address from being offered.

grace period

When a DHCP client actively releases a lease, or when the lease expires without being renewed by the client, the DHCP server does not immediately delete the lease record and return the associated IP address to the available address pool. A grace period is the interval of time for which the lease record is retained before the DHCP server automatically deletes the record from its lease list, thereby making the IP address available for lease assignment to another client. The grace period is not a configurable value. See also the discussion of the grace period and what it means when the DHCP server is running in "View and manage current DHCP leases" on page 168.

reservation

You may use a reservation to create a permanent address lease assignment by the DHCP server. Reservations assure that a specified hardware device on the subnet can always use the same IP address. Address lease reservations associate a specific IP address with a specific client's Ethernet MAC address.

options

Options are other client configuration parameters that the DHCP server can assign when serving leases to DHCP clients. Most options are defined in RFC 2132. The DHCP server in Digi device supports a limited set of options:

- Option 3: Routers on Subnet
- Option 6: DNS Servers

Addresses in the DHCP server settings

The IP address and subnet mask of the DHCP server's scope are the static IP configuration settings for the Digi device itself.

The default gateway (router) provided to a client with the lease information is the IP address of the Digi device.

The DNS servers provided to a client with the lease information are the DNS server addresses configured in the Digi device. These addresses include any DNS server addresses that the Digi device acquires when it connects to the mobile network.

DHCP server configuration settings

Here are the configuration settings for the DHCP server. Typically, these settings can be modified without having to restart the DHCP server for the changes to become effective in the running server.

- **Enable Dynamic Host Configuration Protocol (DHCP) Server:** Enables the DHCP server feature on this Digi device. Note that for the DHCP server to operate, the Digi device must be configured to use a static IP address. For information on how to configure static IP settings, see "Ethernet IP settings" on page 65.
- **IP Addresses:** The starting and ending IP addresses for the scope being served by this DHCP server. These addresses must be in the same subnet as the Digi device itself.
- **Lease Duration:** The length of the leases for the scope being served by this DHCP server. The default lease duration is 24 hours. A DHCP client may request a lease duration other than this setting, and the DHCP server will grant that request if possible.
- **Wait specified delay before sending DHCP offer reply:** The interval of time in milliseconds to delay before offering a lease to a new client. The default delay is 500ms, and the range is 0 to 5000ms. Use of this delay permits this Digi device to reside on a network with other DHCP servers, yet not offer leases to new clients unless the other DHCP servers do not make such an offer. This provides a measure of protection against inadvertently connecting a Digi device to a network that is running its own DHCP server(s), and offering leases to clients in a manner inconsistent with that network.
- **Check that an IP address is not in use before offering it:** When a DHCP client requests a new IP address lease, before offering an IP address to that client, use “ping” to test whether that IP address is already in use by another host on the network but is unknown to the DHCP server. If an IP address is determined to be in use, it is marked as **Unavailable** for a period of time, and it will not be offered to any client while in this state. Enabling this test adds approximately one second of delay before the IP address is offered to the client, since the “ping” test must not receive a valid reply for that test to successfully determine that the IP address is not already in use. This option is off (disabled) by default. This option does not apply to Static Lease Reservations, since the “ping” test is not used for them.
- **Static Lease Reservations:** A static lease reservation is a specific IP address paired with a client's MAC address, which reserves the IP address for that client's use only. This assures that a client always receives a lease for the same IP address and that no other client obtains a lease for that address.

To add a reservation, enter the IP Address and MAC Address values, check or clear the **Enable** checkbox, and then press the **Add** button.

After adding a reservation, you may click on the IP address or MAC address of that entry in the table, permitting you to specify or modify the lease duration for this reservation.

The **Enable** checkbox for the entry permits a reservation to be disabled without actually removing the entry, then enabled again at a later time.

The **Remove** link is used to permanently remove a reservation from the DHCP server configuration.

The **Remove All** link is used to permanently remove all reservations from the DHCP server configuration.

- **Address Exclusions:** A specific set of IP addresses to exclude from the scope. The DHCP server will not grant leases to clients for any IP address in the exclusion range.

  To add an exclusion, enter the starting and ending IP Addresses, check or clear the **Enable** checkbox, and then press the **Add** button.

  The **Enable** checkbox for the entry permits an exclusion to be disabled without actually removing the entry, then enabled again at a later time.

  The **Remove** link is used to permanently remove an exclusion from the DHCP server configuration.

  The **Remove All** link is used to permanently remove all exclusions from the DHCP server configuration.

- **Apply button:** You **must** click the **Apply** button to save changes you make to the DHCP server settings. If you leave this page without applying the changes, those changes will be discarded.

Manage the DHCP server

For information on managing the DHCP server and viewing and managing lease status, see "Manage DHCP server operation" on page 167.

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 interface. Disabling basic services such as Telnet, Rlogin, etc. can make the Command-Line interface inaccessible.

Supported network services and their default network port numbers

In Digi devices 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
```

Manuals ID 6-01

The table shows network services, 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 devices 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 device 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 device 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 device and access the command-line interface through Rlogin.	513
Remote shell (Rsh)	Allows users to log in to the Digi device and access the command-line interface through Rsh.	514
Secure Shell (SSH)	Allows users secure access to log in to the Digi 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 devices.	2601
Simple Network Management Protocol (SNMP)	Managing and monitoring the Digi 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

Service	Services provided	Default network port number
Telnet Server	Allows users an interactive Telnet session to the Digi device's command-line interface. If disabled, users cannot Telnet to the device.	23
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 interface 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

Network services and IP pass-through

The IP pass-through feature (**Configuration > Network > IP Pass-through**) causes the Digi device to be bridged transparently between the Ethernet and mobile data links. Enabling IP Pass-through disables many device features, including many network services. To provide access to the device for configuration and management purposes, you can configure a subset of network services to terminate at the Digi device instead of being passed on to a connected device such as a router. In the IP pass-through feature, these network services are called *pinholes*. Services that can be configured as pinholes include HTTP, HTTPS, Telnet, SSH, and SNMP. See "Virtual Private Network (VPN) settings" on page 77 for more information.

Dynamic DNS update settings

A Dynamic DNS (DDNS) service allows a user whose IP address is dynamically assigned to be located by a host or domain name. Before a DDNS service may be used, you must create an account with the DDNS service provider. The provider will give you account information such as username and password. You will use this account information to register your IP address and update it as it changes.

A DDNS service provider typically supports the registration of only public IP addresses. When using such a service provider, if your Digi device has a private IP address (such as 192.168.x.x or 10.x.x.x), your update requests will be rejected.

The Digi device monitors the IP address it is assigned. It will typically update the DDNS service or server automatically, but only when its IP address has changed from the IP address is previously registered with that service.

DDNS service providers may consider frequent updates to be an abuse of their service. In such a circumstance, the service provider may act by blocking updates from the abusive host for some period of time, or until the customer contacts the provider. Please observe the requirements of the DDNS service provider to ensure compliance with possible abuse guidelines.

The Dynamic DNS Update Settings page includes both settings and status information.

Settings

- **Use the following dynamic DNS service:** Disables DDNS updates, or selects the DDNS service provider to use to register the IP address of this Digi Cellular Family device. When you select a specific DDNS service provider, you must also provide the related account information for that service provider.

  To force an update request to be sent to a particular DDNS service.

  1. Select the "None" radio button to disable DDNS updates, and then click the **Apply** button to save that change.
  2. Select the radio button for the DDNS service you wish to update
  3. Click **Apply** to save that change.

     If the settings for the selected DDNS service are all specified and valid, an update request will be sent immediately to that service.

- **DynDNS.org DDNS Service:** You must create your account at DynDNS.org before you can successfully register the IP address of your Digi device with their service. Please familiarize yourself with their service options and requirements, in order to most effectively use this feature of your Digi device.

  This DDNS service supports only public IP addresses. If you have a private IP address (such as 192.168.x.x or 10.x.x.x), your update requests will be rejected.

- **Host and Domain Name:** The fully qualified host and domain name you have registered with your service provider. An example is: myhost.dyndns.net.
- **DynDNS User Name:** The user name for the account you have created with your service provider.
- **DynDNS Password:** The password for the account you have created with your service provider.

- **DynDNS DDNS System:** The system for the account you have created with your service provider. DynDNS.org supports a number of different services, which vary by the system you select. The available choices are:
  - Dynamic DNS
  - Static DNS
  - Custom DNS
- **Use Wildcards:** Enables/disables wildcards for this host. The available choices for this option are:
  - Disable wildcards
  - Enable wildcards
  - No change to service setting

  According to wildcard documentation at DynDNS.org: "The wildcard aliases *.yourhost.ourdomain.tld to the same address as yourhost.ourdomain.tld."

  Using this option in the settings for your Digi device has the same effect as selecting the wildcard option on the DynDNS.org website. To leave the wildcard option unchanged from the current selection on their web site, use the "no change" option in the device settings. Note that DynDNS.org support for this option may vary according to the DynDNS system you are registered to use.
- **Connection Method:** The connection method to try when connecting to your service provider to register your IP address. DynDNS.org supports three methods to connect. The available choices are:
  - Standard HTTP port 80
  - Alternate HTTP port 8245
  - Secure HTTPS port 443

Status and history information

Following the settings are status and history information for the DDNS service.

- **Most Recent DDNS Service Update Status:** This section provides the status of the most recent attempt to update a DDNS service or server. The displayed information confirms the success of an update request, or it may offer information as to the reason an update request was rejected by the service or server.

  A number of status items are shown. Some of them are specific to the DDNS service being updated. Such information will be helpful when trying to resolve update failures with the DDNS service provider.
  - **Service:** The name of the DDNS service provider or server being updated.
  - **IP Address Reported:** The IP address for your Digi device that is being registered with the DDNS service provider or server.
  - **Update Status:** A simple indication of success or failure for this last update request.
  - **Result Information:** A DDNS service-specific status message, helpful when consulting technical support.
  - **Raw Result Data:** DDNS service-specific update result data returned by the service provider, helpful when consulting technical support.

- **Last Logged Action or Result (may be helpful for troubleshooting):** The last attempted, logged action or result for the DDNS feature, helpful for troubleshooting possible problems with DDNS updates. This information may help identify problems with settings, network connection failures, and other issues that prevent a DDNS update from being completed successfully. Successful results also are reported here.

IP filtering settings

You can better restrict your device on the network by only allowing certain devices or networks to connect. This is better known as IP Filtering or Access Control Lists (ACL). By enabling IP filtering, you are telling the device to only accept connections from specific and known IP addresses or networks. Devices can be filtered on a single IP address or can be restricted as a group of devices using a subnet mask that only allows specific networks to access to the device.

Caution It is important to plan and review your IP filtering settings before applying them. Incorrect settings can make the Digi device inaccessible from the network.

On the IP Filtering Settings page, enter the settings as follows:

- **Only allow access from the following devices and networks:** Enables IP filtering so that only the specified devices or networks are allowed to connect to and access the device. Note that if you enable this feature and the system from which you are connecting to the Digi device is not included in the list of allowed devices or networks, then you will instantly no longer be able to communicate or configure the device from this system.
- **Automatically allow access from all devices on the local subnet:** Specifies that all systems and devices on the same local subnet or network of the device should be allowed to connect to the device.
- **Allow access from the following devices:** A list of IP addresses of systems or devices that are allowed to connect to this device.
- **Allow access from the following networks:** A list of networks based on an IP address and matching subnet mask that are allowed to connect to this device. This option allows grouping several devices that exist on a particular subnet or network to connect to the device without having to manually specific each individual IP address.

IP forwarding settings

When a Digi device acts as a router and communicates on both a private and public network with different interfaces, it is sometimes necessary to forward certain connections to other devices. This is also known as Network Address Translation (NAT) or Port Forwarding. When an incoming connection is made to the device on the private network, the IP port is searched for in the table of port forwarding entries. If the IP port is found, that connection is forwarded to another specific device on the public network.

Port Forwarding/NAT is useful when external devices can not communicate directly to devices on the public network of the Digi device. For example, this may occur because the device is behind a firewall. By using port forwarding, the connections can pass through the networks transparently. Also, Port Forwarding/NAT allows multiple devices on the private network to communicate to devices on the public network by using a shared private IP address that is controlled by Port Forwarding/NAT.

Port forwarding can be used to connect from a Digi device to a RealPort device, such as a Digi Connect SP. For this type of connection to occur, your mobile wireless provider must be mobile-terminated.

IP Forwarding settings include:

- **Enable IP Routing:** Enables or disables IP forwarding.
- **Apply the following static routes to the IP routing table:** The Digi device can be configured with permanent static routes. These routes are added to the IP routing table when this device boots, or afterward when network interfaces become active or changes are made to this list of static routes. The use of static routes provides a means by which IP datagrams can be routed to a network that is not a local network or accessible through the default route.
- **Enable Network Address Translation (NAT):** Enables or disables the use of NAT.
- **Forward protocol connections from external networks to the following internal devices:** Enables protocol forwarding to the specified internal devices. Currently, the only IP protocols for which protocol forwarding is supported are:
  - Generic Routing Encapsulation (GRE, IP protocol 47)
  - Encapsulating Security Payload (ESP, IP protocol 50, tunnel mode only).

  These are routing protocols that are used to route (tunnel) various types of information between networks. If your network needs to use the GRE or ESP protocol between the public and private networks, enable this feature accordingly.
- **Forward TCP/UDP connections from external networks to the following internal devices:** Specifies a list of connections based on a specific IP port and where those connections should be forwarded to. Typically the connecting devices come from the public side of the network and are redirected to a device on the private side of the network.

Example

For example, to enable port forwarding of RealPort data (network port 771) on a Digi Connect WAN VPN to a Digi Connect SP with an IP address of 10.8.128.10, you would do the following:

- Make sure the **Enable IP Routing** checkbox is checked.

- In the **Forward TCP/UDP connections from external networks to the following internal devices** section**,** enter the port forwarding information as follows, and click **Add**:

Socket tunnel settings

A Socket Tunnel can be used to connect two network devices: one on the Digi 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 device device on the configured port number. The Digi device then opens a separate connection to the specified destination host. Once the tunnel is established, the Digi 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 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 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 device will use to make a connection to the destination device.
- **Destination Protocol:** This is the protocol used between Digi 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.

Virtual Private Network (VPN) settings

Virtual Private Networks (VPNs) are used to securely connect two private networks together so that devices may connect from one network to the other network using secure channels.VPN uses IP Security (IPSec) technology to protect the transferring of data over the Internet Protocol (IP). All Digi Cellular Family products except Digi Connect WAN support VPNs.

The Digi device is responsible for handling the routing between networks. Devices within the private network served by the Digi device can connect directly to devices on the other private network to which the VPN tunnel is established to. The VPN tunnels are configured using various security settings and methods to ensure the networks are secured.

Uses for VPN-enabled Digi devices

VPN-enabled Digi devices, such as Digi Connect WAN VPN, are cellular-enabled routers that securely connect remote subnets using IPsec VPN technology. Devices in the Digi device's private network can connect directly to devices on the other private network with which the VPN tunnel is established. You configure VPN tunnels using security settings and methods to ensure the networks are secured.

The Digi device is used for primary or backup remote site connectivity. Secured IPsec VPN traffic is typically routed from the Digi device over the cellular IP network and is terminated by a VPN appliance at the host end.

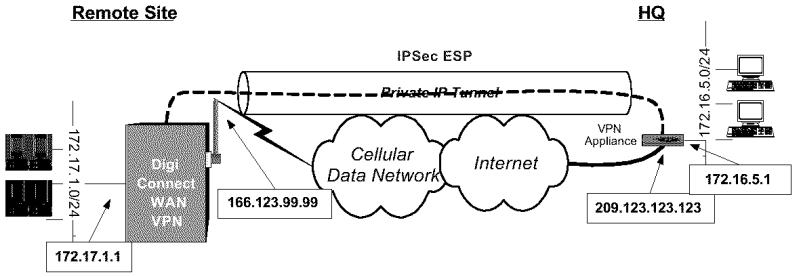
A VPN-enabled Digi device can be used in several scenarios; for example:

- As the *primary* remote site router where no other WAN router is used.
- As a *backup* router where the remote site has a primary WAN connection through DSL, Frame Relay, or other means.
- To provide secure access to remote serial and/or Ethernet devices.

This section describes using a Digi device as a *primary* remote site router using IPsec Encapsulated Security Payload (ESP) and Internet Key Exchange (IKE)/Internet Security Association and Key Management Protocol (ISAKMP) pre-shared key methods.

Example VPN configuration

The diagram shows a Digi Connect WAN VPN used as a primary remote site router:



How VPN tunnels work

The Digi device's Ethernet port usually connects to a switch or hub, which then connects to other Ethernet devices. The mobile/cellular carrier provides only one IP address to the mobile interface. The Digi device uses Network Address Translation (NAT), where only the mobile IP address is visible to the outside. Private IP addresses are typically used on the remote site LAN connected to the Digi device's Ethernet port. All outgoing traffic, except the tunneled VPN traffic, uses the mobile IP address of the Digi device. Using the example network above, the process for initiating VPN tunnels works like this:

1. Typically, a host or device on the remote subnet (in this case, 172.17.1.0) requests information from a host on the main site (HQ) subnet (172.16.5.0). For example, a computer at 172.17.1.20 needs a file from 172.16.5.100.
2. The Digi device sees the request as being on the HQ subnet and checks whether a VPN tunnel exists between the two sites.
3. If no tunnel exists, the Digi device initiates a VPN tunnel request to its peer — the VPN concentrator at HQ. The VPN policy settings are compared, and if they match, an IPsec tunnel is created between the Digi device and the VPN concentrator. Traffic is encrypted as defined in the VPN policies. The maximum number of supported tunnels is two.

IP address requirements for VPN tunnels

To establish an IPSec VPN tunnel, the IP address of the mobile interface must be publicly accessible. The IP address can be either static or dynamic depending upon the requirements of your VPN end point. The IP address, however, cannot be within a private range of addresses (for example, 10.0.0.0, 172.16.0.0 or 192.168.0.0). If the mobile IP address is within one of the private IP address ranges, the mobile carrier is using a NAT (Network Address Translation) server between your mobile IP address and the internet. The Digi Connect WAN VPN does not currently support NAT-Traversal.

GSM GPRS/EDGE APN type needed

If the VPN end points require static (persistent) IP addresses, you may need a custom access point name (APN). An Internet APN can work in these cases:

- The main site (HQ) VPN appliance can support Dynamic DNS names.
- Another form of authentication is used (for example, FQDN).

Be aware that these APNs are based on Cingular Blue; other carrier APNs may have similar requirements.

CDMA carrier requirements

The CDMA (Code-Division Multiple Access) carrier requirements are similar to GSM in that static IP addresses may be required depending on the host site concentrator VPN implementation. In both cases, the Digi device's mobile IP address will likely need to support mobile terminated data; that is, the ability to accept incoming data connections.

HQ router / VPN appliance configuration

For supported protocols, see the IPsec specifications your Digi device.Security policies on the HQ VPN device must match those on the Digi device. The HQ VPN appliance's peer address is the Digi device's mobile IP address.

Using a console port

The Digi device's console port can be configured for Console Management to provide SSH or Telnet access. It can be cabled to the router or VPN appliance's console port to provide true diverse out-of-band console access.

Configure VPN settings

This procedure shows how to configure the VPN connection from the web interface (**Configuration > Network > Virtual Private Network (VPN) Settings**). In the command-line interface, the "set vpn" command configures VPN connections, and the "vpn" command manages them. Generally, configuring VPN connections from the web interface is simpler. Review the settings descriptions in this procedure (also available in the online help) to determine whether you need to gather any information before you start setting up the VPN.

Configuration settings used in this example

This procedure uses an example configuration, where an IPsec ESP uses an Internet Key Exchange/ISAKMP pre-shared key. The IP addresses used in the instructions are examples only. Settings used in the example are:

Setting	Remote Site (Digi Connect VPN)	HQ (VPN Concentrator)
Local Interface IP address	172.17.1.1	172.16.5.1
Local Subnet	172.17.1.0/24	172.16.5.0/24
External/Mobile IP address	166.213.99.99	209.123.123.123
Remote Subnet	172.16.5.0/24	172.17.1.0/24
Remote VPN Endpoint	209.123.123.123	166.123.99.99
ISAKMP Shared Secret	sixteencharacter	sixteencharacter
Identity: User FQDN	vpntest@digi.com	vpntest@digi.com
IKE parameters	DES / MD5 / 86400 sec.	DES / MD5 / 86400 sec.
IPsec parameters	3DES / MD5 / 86400 sec.	3DES / MD5 / 86400 sec.

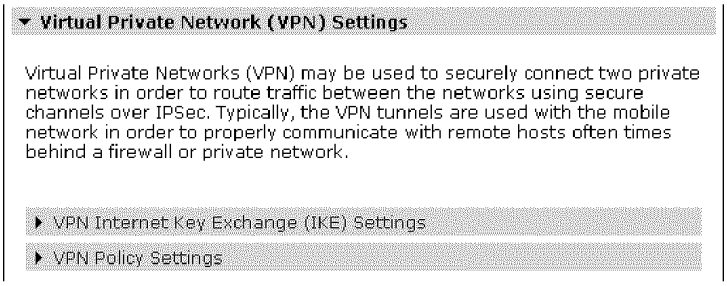
Manuals ID 6-01

1 Assign a static IP address to the Ethernet port. The default IP address for the Ethernet port is 1**92.168.1.1**. The default gateway may change to an address such as 10.6.6.6, which is the mobile service provider's default gateway.

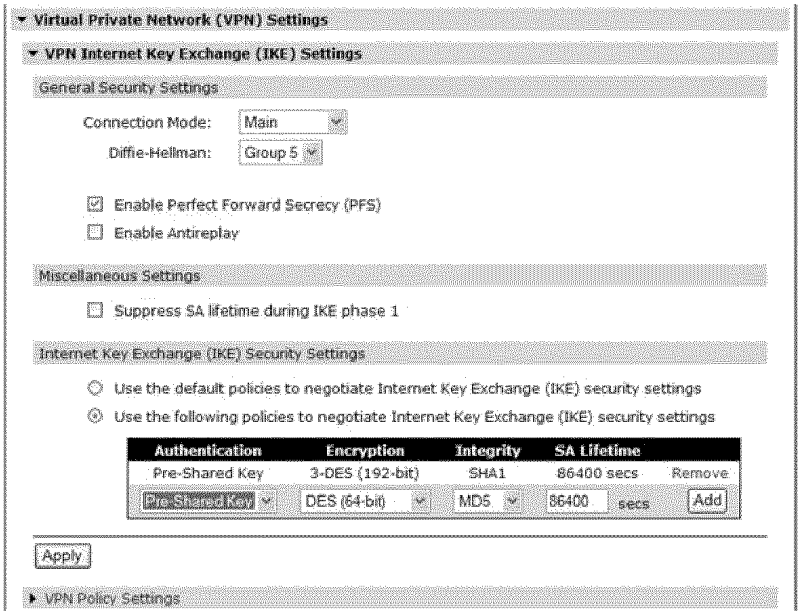
2 Using a web browser, open the web interface for the Digi device using the its assigned IP address; for example, 172.17.1.1.

3 From the main menu, go to **Configuration > Network > Virtual Private Network (VPN) Settings**. There are two groups of VPN settings:

- **VPN Internet Key Exchange (IKE) Settings:** These settings define the identity, general security, and Internet Key Exchange security settings for the VPN connection.
- **VPN Policy Settings:** These settings define the VPN tunnels and their security settings.



4 Click **VPN Internet Key Exchange (IKE) Settings.**



There are several groups of settings on the **VPN Internet Key Exchange (IKE) Settings** page:

General Security Settings:

– **Connection Mode:** The method in which Internet Key Exchange (IKE) phase one negotiations is completed. IKE phase one negotiations are used to establish the various security settings and establish a secure channel for subsequent messages.The default is Main Mode.

  Main Mode: Processes phase one negotiations with three 2-way exchanges between the VPN client and remote VPN endpoint. The exchanges are meant to match Internet Key Exchange Security Associations (SA) between peers to provide a protected pipe for subsequent protected ISAKMP exchanges between the peers. The first exchange is responsible for negotiating and agreeing upon the algorithms and hashes/keys used to secure the Internet Key Exchange communications. The second exchange uses a Diffie-Hellman exchange per the specified Diffie-Hellman group to generate nonces and shared secret keys in order to sign and prove identities. The third exchange verifies the identity per the specified Identity.

  Aggressive Mode: Processes phase one negotiations with fewer exchanges than Main Mode. In the first exchange, almost everything is sent in the proposed Internet Key Exchange values including the Diffie-Hellman key, nonce to sign and verify, and the identity. The weakness of using Aggressive Mode compared to Main Mode is that negotiations exchange information before the secure channel is created. However, because less exchanges are used, aggressive mode is faster than main mode.

– **Diffie-Hellman:** Diffie-Hellman is a public-key cryptography protocol for establishing a shared secret over an insecure communications channel. Diffie-Hellman is used within Internet Key Exchange to establish the session keys that create a secure channel. The method and security factor used to control the exchange is specified by the Diffie-Hellman group. The greater the group, the more secure the transaction. However, because the keys and cryptography calculations are larger, they also require more processing time and performance costs. The default is Group 2.

  Group 1 (768-bit): Uses a 768-bit Diffie-Hellman prime modulus group to secure the shared secret.

  Group 2 (1024-bit): Uses a 1024-bit Diffie-Hellman prime modulus group to secure the shared secret.

  Group 5 (1536-bit): Uses a 1536-bit Diffie-Hellman prime modulus group to secure the shared secret

– **Enable Perfect Forward Secrecy (PFS):** Perfect Forward Secrecy establishes greater resistance to cryptographic attacks by ensuring that a given key of an Internet Key Exchange SA is not derived from any other secret, and that no other key can be derived from this key. Set this field to match that at the remote VPN gateway. Default is Enabled.

– **Enable Antireplay:** Antireplay allows the IPsec tunnel receiver to detect and reject packets that have been replayed.Set this field to match that at the remote VPN gateway. The default is Enabled.

  Important: Disable Antireplay if you use manual keyed tunnels.

Miscellaneous Settings:

Suppress SA lifetime during IKE Phase 1: In most cases, leave this option unchecked . Some VPN equipment does not negotiate the ISAKMP Phase 1 lifetimes. Such equipment may refuse to negotiate with the Digi device if it includes lifetime values in Phase 1 negotiation messages. If the Digi device must communicate with such equipment, enable this option to prevent the Phase 1 lifetimes from being included in the ISAKMP Phase 1 messages.

Internet Key Exchange (IKE) Security Settings: These settings negotiate IPSec security associations (SA). The IPSec systems must authenticate themselves to each other and establish ISAKMP (IKE) shared keys. SAs are relationships between two or more entities or peers that describe how they will use security services to communicate securely.

Use either the default security policies or custom policies.

– **Use the default policies to negotiate Internet Key Exchange (IKE) security settings:** The default security policies that are negotiated and used to secure the SAs are:

– **Use the following policies to negotiate Internet Key Exchange (IKE) security settings:** If the default settings do not match the VPN and IKE SA configuration of the remote peers, or if additional policies are required, enable this setting, then click **Add** to add one or more security policies.

Internet Key Exchange security policy settings include:

Authentication: The authentication algorithm used in IKE negotiations to authenticate IKE peers and SAs. Supported authentication algorithms are MD5 and SHA1.

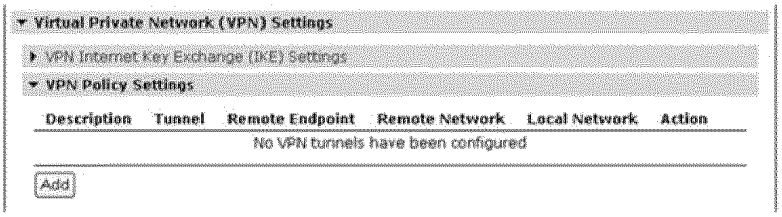
Encryption: The encryption algorithm and key length used in IKE negotiations for encrypting data. Supported encryption algorithms are DES, 3-DES, and AES, which also includes three available key lengths for greater security.

Integrity:

SA Lifetime: Determines how long a SA policy is active in seconds. The Security Association (SA) lifetime determines how long a SA policy is active in seconds. After the IKE SA has been negotiated, the SA lifetime begins. Once the lifetime has completed, a new set of SA policies are negotiated using IKE phase 2 negotiation.

When all the VPN Internet Key Exchange settings have been entered, click **Apply**.

5 Click **VPN Policy Settings** to add, modify, or delete a VPN tunnel. VPN Tunnels define the actual tunnels between two private networks. The tunnels specify the information required to establish the secure channel, the routing between networks, and the security policies used to encrypt and authorize the data. You can create a maximum of two tunnels.If there are no VPN tunnels defined, the page looks like this:



- To **add** a new VPN tunnel, click **Add**. If **Add** is disabled, the maximum tunnels have already been created, and you can only modify or remove them.
- To **modify** an existing VPN tunnel, click the tunnel's index number in the Tunnel column.
- To **remove** an existing VPN tunnel, select the tunnel and click **Remove**.

VPN Tunnel #*n* - Configuration settings: For each VPN tunnel, there is a page of configuration settings. These settings typically are specified by the remote VPN server and should correspond accordingly.

- **Description:** A description or name for the VPN tunnel.
- **Remote VPN Address:** The IP address or hostname of the peer with which to establish the connection.
- **VPN Tunnel:** The method of establishing the VPN tunnel. Tunnels can be either Manual-Keyed IPSec/ESP or ISAKMP.

  Manual-Keyed IPSec/ESP tunnels are established by manually specifying the tunnel and security settings. See page 89 for more information on these tunnels.

  ISAKMP tunnels are established by specifying list of security policies in order to negotiate a set of security settings from the remote VPN endpoint. Use ISAKMP whenever the remote gateway supports it. ISAKMP tunnels are usually easier to set up than a manually-keyed tunnel and are more secure. See page 91 for more information on these tunnels.

- **Local Endpoint Type:** Set this field to reflect how the local end of the VPN tunnel is terminated. The local end can be a subnet or an internal interface.

  Local endpoint is a subnet: Select this type of endpoint to make the VPN tunnel directly connect a subnet on the local network with a subnet on a remote network. Devices on the remote network will be able to see the IP addresses of devices on the local network.

  Local endpoint is an internal interface: Select this type of endpoint to hide the IP address of devices on the local network from devices on the remote network. In this mode of operation, the local side of the VPN tunnel is terminated at a virtual network interface, internal to the Digi device. You set the IP address of this interface. This mode of operation is used in combination with NAT. When devices on the local network send data to the remote network, the data packets are processed by NAT, which changes the source address to that of the virtual interface. When devices on the remote network send data back, they send it to the address of the virtual interface. NAT changes the destination address of these packets to be the correct addresses on the local network. For information on the Network Address Translation (NAT) settings, see "IP forwarding settings" on page 75.
- **Identity settings:** These settings specify how the VPN client and its security settings will be identified to the remote VPN endpoint. These settings must match the identity settings provided by the remote VPN endpoint to properly identify this client and its security settings. The identity can be defined as a string, an IP address, or through an X.509 identity certificate. e

  Network Interface: Select the network interface that should be used as the local endpoint of the VPN tunnel. This interface will be used to communicate with the remote VPN peer. In most cases, you should set this field to mobile0.

  Negotiate tunnel as soon as interface comes up: Check this field to force the system to negotiate the VPN tunnel as soon as the selected network interface is ready for use. Uncheck this field to make the system wait until it receives packets directed to the remote network before negotiating the VPN tunnel.

  Use the following as the identity: An identity string that identifies the VPN client with the remote VPN endpoint. The default is *macaddress*@digi.com; that is, the MAC address for the Digi device. You can also specify the identity as:

  A **Fully Qualified Domain Name** (FQDN): Usually the FQDN of the Digi Connect device. For example: www.myhost.com

  A **User FQDN**: Similar to standard FQDN but with a user name. The format is the same as an email address. For example: user@myhost.com

  A **Network Address** (IPv4): A standard IP address (version 4) that uses the standard IPv4 dotted format (four numeric values between 0 and 255 separated by periods). For example: 10.0.0.1

  Use the interface IP address: The IP address of the network interface selected for the VPN tunnel will automatically be used as the VPN identity.

  Use the identity certificate X.509 distinguished name (DN): Choose this setting if VPN identity and certificate key files are being used to manage VPN identity and security. See Administration > X.509 Certificate/Key Management for those settings.

- **Local Endpoint settings:**

  Tunnel Network Traffic from the following Local Network IP Address
  Subnet Mask: The routes required to access clients on the local network and the clients that are allowed to access the remote clients through the VPN tunnel. These routes are specified using the local network IP address and subnet mask.

  Tunnel Network Traffic from the following Local Network IP Address
  Subnet Mask: The routes required to access clients on the remote network and the remote peers to which local clients are allowed to connect. These routes are specified using the remote network IP address and subnet mask.

- **Incoming/Outgoing Traffic Security Settings** (for Manual Keyed VPN tunnels)**:**
  or
  Security Settings: (for ISAKMP VPN tunnels):
  Depending on the method chosen for establishing the tunnel in **VPN Tunnel**, security settings for the tunnel are displayed.

  Manual-Keyed tunnels specify the tunnel and security settings manually. These settings must match the settings of the remote VPN endpoint. See page 89 for descriptions of these settings.

  ISAKMP tunnels use a pre-shared key and a a list of security policies used to negotiate security settings. See page 91 for descriptions of these settings.

- **Local Endpoint:** These settings depend on the selection for Local Endpoint Type.

  If the **Local Endpoint Type** is **Local endpoint is a subnet,** enter the IP address and subnet mask of the local endpoint. The Local Network settings specify the routes required to access clients on the local network. They also specify clients allowed to access the remote clients through the VPN tunnel. Typically, the local network specifies the same network and subnet that the Digi device server is connected to. Thus, any client on the same network can communicate over the VPN tunnel.

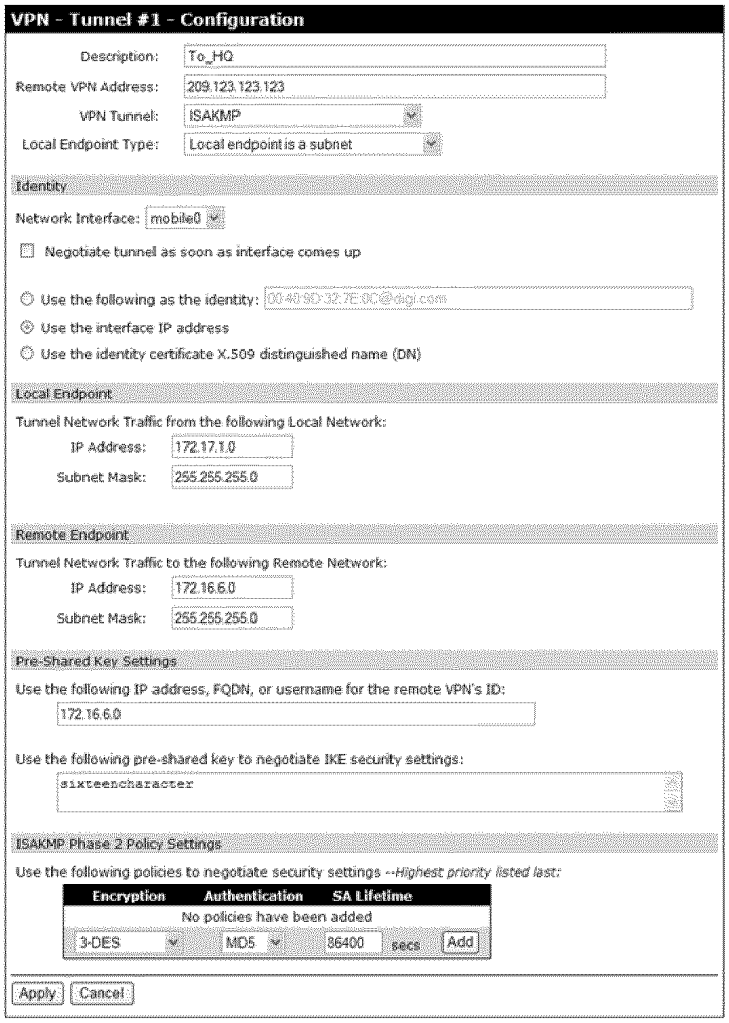
  If the **Local Endpoint Type** is **Local endpoint is an internal interface,** specify the endpoint by entering the IP address that will be assigned to the endpoint's internal interface. This address should not be within any local or remote network addressable by the Digi device server. Packets sent to the remote network are processed by NAT, which sets the source address of these packets to this IP address. All packets sent through the VPN tunnel will appear, to devices on the remote network, to come from this IP address. Devices on the remote network will send their data to this IP Address.

  Check the **Discard packets...** field to make the Digi device server discard any packets sent to the tunnel's remote subnet that do not come from the local subnet which you specify in the prompts immediately below.

- **Remote Endpoint:** These settings specify the routes required to access clients on the remote network. They also specify the remote peers that local clients are allowed to connect to. Typically, the remote VPN endpoint is connected to both a public network (the remote VPN endpoint address) and a private network. The remote network specifies the private network that the remote VPN endpoint is connected to.

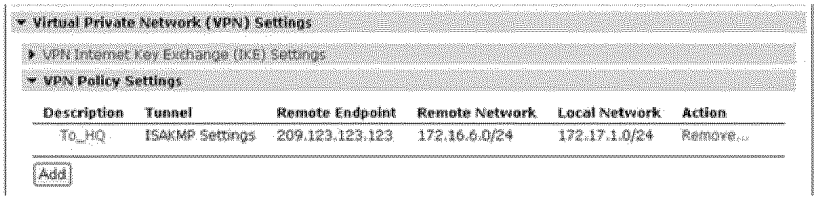
When all VPN tunnel settings are entered, click **Apply**.

For example, to configure the ISAKMP VPN tunnel in the example configuration, choose **ISAKMP** and enter the pre-shared key (PSK) information and security policy.



When the VPN tunnel has been added to the configuration settings after you click **Apply**, the VPN Policy Settings page looks like this:

6 Configure the remote VPN concentrator with the same settings, remembering to reverse the



peer endpoint and remote/local subnet settings.

7 To test the VPN connection, generate traffic from the remote subnet to the HQ subnet.

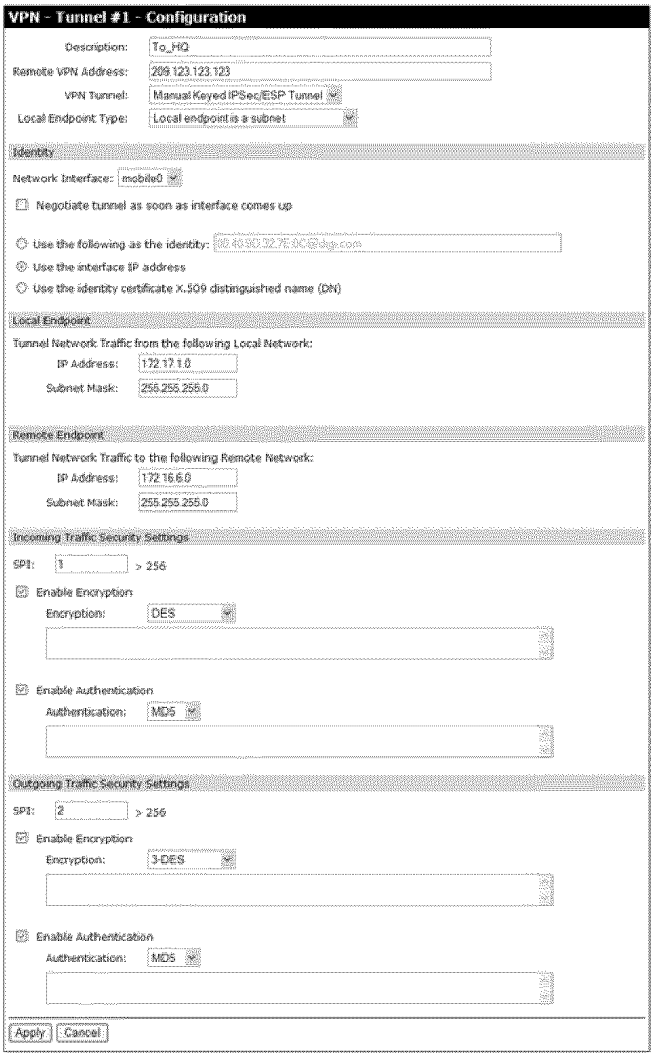
For example, from 172.17.1.100, ping 172.16.5.1. The response from the first few pings will be “Destination Host Unreachable” because 172.17.1.100 does not know the route to the remote site. After the VPN tunnel is established, the ping either responds or times out.

8 To manage an active VPN connection, see "Manage Virtual Private Network (VPN) connections" on page 166.

Manuals ID 6-01

Manual-keyed IPSEc/ESP VPN tunnel security settings

Manual-keyed IPSec/ESP tunnels specify the tunnel and security settings manually. You must configure the settings to match those on the remote VPN server. These settings affect the network traffic between the local and remote peers specified on the settings **Tunnel Network Traffic from the following Local Network** and **Tunnel Network Traffic to the following Remote Network**.



There are two groups of manual-keyed settings, for incoming and outgoing traffic, which differ from each other, depending on the implementation of the remote VPN server.

- **Incoming Traffic Security Settings:** Incoming traffic is any traffic sent from a remote peer on the remote network of the remote VPN endpoint to a local peer on the local network.
- **Outgoing Traffic Security Settings:** Outgoing traffic is any traffic sent from a local peer to a remote peer.

The settings for incoming and outgoing traffic are:

- **SPI (Security Parameter Index):** A unique index for a tunnel used to identify the security settings for IPsec. The SPI is a 32-bit unsigned value that must not be less than 256.
- **Enable Encryption**
  Encryption algorithm
  Encryption key: The optional encryption algorithm and associated encryption key used to encrypt data on the VPN tunnel. To specify encryption, check **Enable Encryption** and select the matching encryption algorithm. Enter the encryption key according to the encryption algorithm.Specify either an ASCII value using alphanumerics or a hexadecimal value prefixed by 0x. The encryption key length depends on the encryption algorithm:

Algorithm	Size	Key Length	
		ASCII	Hexadecimal
DES	64-bit	8	16
3 DES	192-bit	24	48
AES	128-bit	16	32

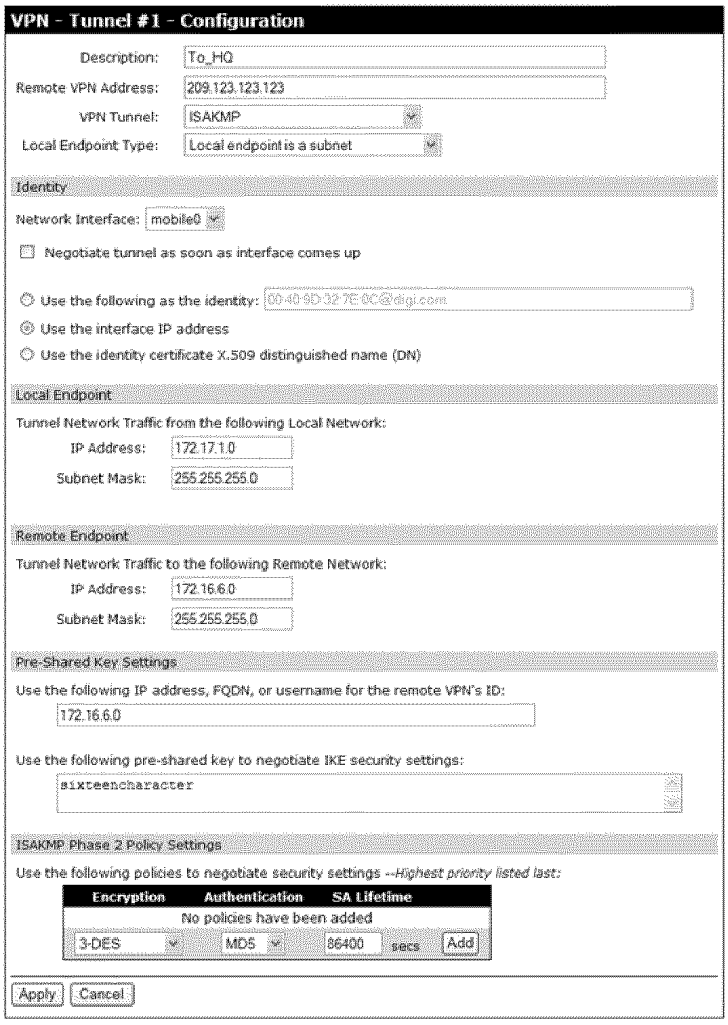
- **Enable Authentication**
  Authentication algorithm
  Authentication key: The optional authentication algorithm and associated authentication key used to authorize access on the VPN tunnel. To specify authentication, check **Enable Authentication** and select the matching authentication algorithm. Enter the authentication key according to the authentication algorithm. Specify either an ASCII value using alphanumerics or a hexadecimal value prefixed by 0x. The authentication key length depends on the authentication algorithm:

Algorithm	Size	Key Length	
		ASCII	Hexadecimal
MD5	128-bit	16	32
SHA1	160-bit	20	40

ISAKMP VPN tunnel security settings

Configuring an ISAKMP VPN tunnel requires several settings to be set as specified by the remote VPN server: The local and remote network settings that handle the routing between the local and remote peers, and aset of security policies to define the security settings for incoming and outgoing traffic. Incoming traffic is defined as any traffic sent from a remote peer on the remote network of the remote VPN endpoint to a local peer on the local network. Outgoing traffic is defined as any traffic sent from a local peer to a remote peer.

Manuals ID 6-01



- **Pre-Shared Key Settings:**
  - **Use the following IP address, FQDN, or username for the remote VPN's ID:**
  - **Use the following pre-shared key to negotiate IKE security settings:** The Pre-Shared Key (PSK) specifies the shared key used to secure the VPN tunnel. The key may be specified as an ASCII value using alpha-numeric characters or may be specified as a hexadecimal value prefixed by "0x". The key may be specified as either a 128-bit key, 192-bit key, or 256-bit key. The corresponding key lengths in ASCII and Hexadecimal values are:

- **ISAKMP Phase 2 Policy Settings:**
  - **Use the following policies to negotiate security settings:** Security policies define the set of security settings for incoming and outgoing traffic used to encrypt and authorize data. One or more sets of settings may be specified. The actual set of negotiated settings depends on the available policies specified by the remote VPN endpoint.

    To add a new set of security policies, enter the encryption and authentication algorithms for both incoming and outgoing traffic and click **Add**. When you finish adding the new policies, click **Apply**.

    To modify an existing set of security policies, click any of the corresponding links for the specified policy. When you finish changing the policies, click **Apply**.

    To remove an existing set of security policies, click the **Remove** link for the specified policy. Then click **Apply**.

    Clicking **Apply** is required to save the additions, changes, or removals of security policies.

    For more information, see **VPN tunnel proposal configuration for ISAKMP tunnels** below.

VPN tunnel proposal configuration for ISAKMP tunnels

The Proposal Configuration settings configure a set of security policies for ISAKMP tunnels. The settings define the set of encryption and authentication algorithms for incoming and outgoing traffic over the VPN tunnel. Proposals let you define multiple types of communications. A security policy can have multiple proposals. For example, a security policy can have two proposals to allow older VPN devices to connect using less-secure methods, while allowing the same policy to have a second (or more) proposal to allow newer, more powerful end-points to use more secure methods. For two devices to communicate with each other, they must have a matching proposal.

VPN tunnel proposal configuration settings include:

- **Encryption:** The encryption algorithm used for encrypting data:
  - DES: Uses 64-bit keys
  - 3-DES: Uses 192-bit keys
  - AES: Uses 128-bit, 192-bit, or 256-bit keys depending on the negotiated security settings
- **Authentication:** The authentication algorithm used for authenticating clients:
  - MD5: Uses 128-bit keys.
  - SHA1: Uses 160-bit keys.
- **SA Lifetime:** The Security Association (SA) lifetime determines how long a SA policy is active in seconds. After the SA has been negotiated, the SA lifetime begins. Once the lifetime has completed, a new set of SA policies are negotiated with the remote VPN endpoint.

IP pass-through settings

There are many application scenarios where a router is used to decide upon alternative routes using a primary and a secondary (or backup) interface. In many of these configurations, the router is required to use a public IP address as assigned by the network over which it is communicating. This requirement is mostly owing to the router needing to establish a VPN tunnel over that interface and using the public IP address as part of the VPN authentication. (For more on VPN tunnels, see page 77.)

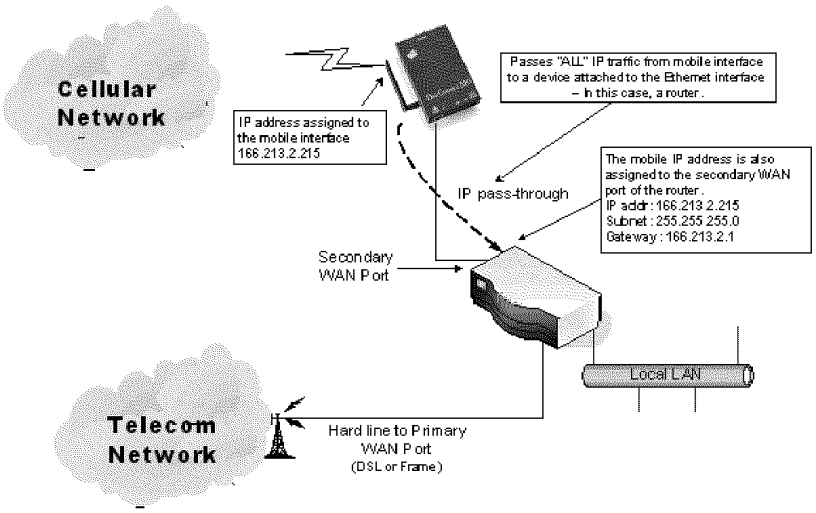
The IP pass-through feature allows a Digi device device to provide bridging functionality similar to that of a cable or DSL modem, where the Digi device becomes "transparent" to the router or connected device. In this case; the router's WAN interface believes it is connected directly to the mobile network and has no knowledge that the Digi device is the mechanism providing that connectivity.

How IP pass-through works

A Digi device configured for IP pass-through, such as a ConnectPort WAN or Digi Connect WAN, passes its mobile IP address directly through and to the Ethernet device (router or PC) to which it is connected through the Ethernet port. From the perspective of the connected device, the Digi device essentially becomes transparent (similar to the behavior of a cable or DSL modem) to provide a bridge from the mobile network directly to the end device attached to the Digi device.

Since the mobile network address is effectively "passed-through" to the local device connected to the Ethernet port of the Digi device, all network access to it is bypassed, with some specific exceptions.

Here is an example of a Digi device configured for IP pass-through in a network with a third-party router.



If the third-party router's WAN interface is attached to the Digi device's Ethernet port, and the Digi device's mobile interface receives the IP address 166.213.2.215, the router's WAN port is assigned the same IP address 166.213.2.215. If the router is receiving the IP address dynamically; the DNS server addresses, subnet mask, and default gateway information will be filled in automatically. If the router is configured manually; you need to obtain the DNS information from the mobile service provider and enter that manually. The subnet mask is 255.255.255.0 and the default gateway is the same as the mobile IP address with ".1" for the last octet. In other words: if the mobile IP address is 166.213.2.215, the default gateway is 166.213.2.1.

IP pass-through's effect on network access to Digi devices

When IP pass-through is enabled, the Digi device effectively disables all router and IP service functionality. Services that are disabled are:

- NAT
- Port Forwarding
- VPN
- DDNS updates
- Socket Tunnel
- Network Services configuration.

The Digi device is effectively transparent to all IP activity and network access by other devices, with these exceptions:

- It can be accessed via the serial port for configuration using the command line interface.
- It accepts TCP/IP connections for purposes of configuration by means of a "pinhole" on the mobile interface.
- It can be accessed by other devices on the local Ethernet segment via the default IP address of 192.168.1.1.

Using pinholes to manage the Digi device

IP pass-through uses a concept called *pinholes*. A Digi device can be configured to listen on specific TCP ports, and terminate those connections at the Digi device for purposes of managing it. Those ports are called pinholes, and they are not passed on to the device connected to the Ethernet port of the Digi device. Network services and ports that can be configured as pinholes include (see "Network services settings" on page 69 to configure these settings):

- Telnet: for accessing the device through a Telnet login and the command-line.
- SSH: for accessing to the device through a Secure Shell (SSH) login and the command-line.
- HTTP: for accessing the device through HTTP and the web interface.
- HTTPS: for accessing to the device through HTTPS and the web interface
- SNMP: for monitoring and managing the device through SNMP.

Connectware Manager and Digi SureLink ports are automatically set up as pinholes so that they continue to work with the Digi device. In addition, the Digi device uses a private address on the Ethernet interface strictly for use in configuration or local access. This allows a user on the local network to gain access to the web interface or a Telnet session in order to make configuration changes.

Remote device management and IP pass-through

As illustrated above, the Digi device allows you to enable pinholes for specific ports to allow remote users to manage the Digi device from the mobile network or open Internet. The Digi device retains its remote management capabilities using Connectware Manager. The necessary pinholes are automatically defined when the Digi device is configured for IP Pass-through.This provides administrators with the same remote-management capabilities that exist in Digi remote devices.

Steps to configure IP pass-through

To configure IP Pass-through from the web interface for your Digi device, follow these steps, or, in the case of the first three steps, make sure they have been performed.

1 Set a static IP address for the Digi device. Go to **Configuration > Network > IP Settings**.

2 Set up the DHCP server. Go to **Configuration > Network > DHCP Server Settings**. See page 65 and the online help for DHCP Server Settings.

3 Turn on the DHCP server. Go to **Management > Network Services.** In **DHCP Server Management,** click the **Start** button.

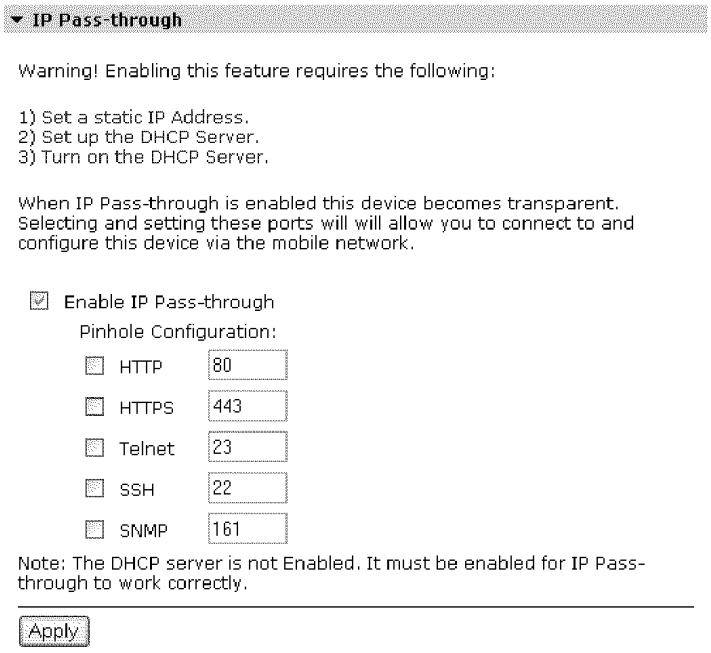
4 Configure IP pass-through settings. Go to **Configuration > Network > IP Pass-through.**

IP pass-through settings include:

- **Enable IP Pass-through:** Enables or disables IP Pass-through.
- **Pinholes:** Specifies whether specific network services/ports are configured as pinholes for purposes of managing the Digi device.

Manuals ID 6-01

The screen shot shows IP Pass-through configuration settings.



Virtual Router Redundancy Protocol (VRRP) settings

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol for routers (but is not a routing protocol)

VRRP allows a number of routers to represent a "virtual router." The virtual router has a unique IP address, and MAC address that can be shared by all routers in a VRRP group. This simplifies configuration of hosts on a network, as they can be configured similarly, without the need to participate in dynamic routing protocols.

There are two roles in VRRP: master, and backup. The master represents the virtual router and forwards IP traffic. Backup routers monitor the health of the master router, and in the event that the master stops sending advertisements, backup routers stage an election to determine which one will be the next master, and take over the virtual router IP address and MAC. The time it takes to make the determination that the master is down, and hold elections depends on configuration, but typically occurs in about 3 seconds. The master can be configured to cause elections to occur based on a number of events (not being able to reach a host, primary link has been lost, etc.). These capabilities are implementation specific. Additionally, if the master router is powered off, or a network cable is removed, and it is no longer able to send advertisements, elections will be held.

A number of VRRP groups (up to 255) can be configured on a LAN. A router may participate in multiple groups. All routers must be within one hop of each other (does not route). VRRP supports IPv4 only, but IPv6 versions are in the works.

Platforms supported on

VRRP is supported on any Digi cellular product (CWAN, CPWAN, CWAN3G, CPX8, CPX4)

Protocol details

VRRP is the most widely supported and deployed router redundancy protocol.

VRRP is an IETF standards-track protocol based on Cisco's proprietary Hot Standby Router Protocol (HSRP). VRRP, however, is not compatible with HSRP.

VRRP was originally defined in RFC 2338 (April 1998), which was made obsolete by RFC 3768 (April 2004).

Where to use

The VRRP feature must be used in conjunction with routers that support the protocol. Many vendors support VRRP (Cisco, Nortel, Juniper, Huawei, Foundry, etc.).

Two or more Digi devices can be used together. For example, you could provide customers with technology diversity by using one Digi on a CDMA network, and another on a GSM network. Carrier diversity could also be implemented in a similar fashion. Customers are already using multiple Digi devices with VRRP.

The Digi device can either be a master or backup, but would most likely be providing cellular backup to a primary router. If the primary router went down or lost link, the Digi would immediately take over routing responsibilities.

Digi could replace or go into applications where a Cisco HWIC is used for backup. The advantage to using a Digi router is that you can place the Digi where the signal is best (vs. having to relocate the Cisco from the wiring closet where the T1, cable, or DSL comes in). Another advantage is

physical redundancy. If the power supply on the Cisco gets fried, or someone spills coffee on it, your HWIC is not going to be of much help.

One limitation of VRRP is that if hosts behind the VRRP router are running a VPN, the VPN must be restarted when a failover occurs. This is not true if the routers are the ones terminating / originating the VPN -- only the hosts.

VRRP is not a routing protocol, and does not distribute information about routes.

- **Virtual Router Identifier (VRID): (1-255)**
- **Priority: (1-254)**
- **Advertisement Interval: msecs**
- **Virtual Router's IP Address**:
- **Enable Preempt**

Manuals ID 6-01

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.

Configure mobile (cellular) settings

The Mobile Settings pages configure how to connect to mobile (cellular) networks using the mobile connection, including the service provider, service plan, and connection settings used in connecting to the mobile network. If your Digi device has not already been provisioned for use in the mobile network, you can launch a wizard to provision it from these pages. In addition, you can configure settings for Digi SureLink™, a feature that provides an "always-on" mobile network connection to ensure rapid on-demand communication. The SureLink configuration settings allow you to customize how SureLink detects when a connection has been lost, in order to re-establish the link.

Information required from mobile service provider

To connect to the mobile network, you must get a set of network settings from the mobile service provider including service plan and authentication details. For more information, consult the documentation that came with your mobile service provider's information.

Different processes used for CDMA and GSM provisioning

The process for provisioning your device and the settings displayed on the Mobile Configuration page vary according to whether the mobile service provider network used with your Digi Cellular Family product is based on CDMA (Code-Division Multiple Access) or GSM (Global System for Mobile communication).

CDMA-based mobile service providers

Device provisioning for a CDMA-based mobile service provider consists of selecting the service provider from a list and either automatically or manually entering mobile settings provided by the mobile service provider Examples of CDMA-based mobile service providers include Sprint, Verizon, Alltel, and Midwest.

GSM-based mobile service providers

Device provisioning for a GSM-based mobile service provider involves inserting a Subscriber Identity Module (SIM) card into the Digi device, which makes subscription data available in the cellular network. Examples of GSM-based mobile service providers include Cingular, AT&T, and T-Mobile.

Set mobile configuration settings to factory defaults

The **Set to Defaults** button on the Mobile Configuration page sets all the mobile settings to factory defaults and sets the Service Provider selection back to deselected.

Mobile service provider settings

The Mobile Service Provider settings part of the screen identifies the service provider to use in connecting to the mobile network. The information displayed varies by Digi Cellular Family product and whether the remote service provider is GSM- or CDMA-based. Settings that may be displayed on this screen include:

- **Service Provider:** For GSM-based mobile service providers, this is the service provider to use in connecting to the mobile network. The service provider must match the

provider that supplied the SIM card.This must match the provider that supplied the SIM card. (Not displayed for CDMA products.)

- **Service Plan:** For GSM-based mobile service providers, this is the service plan to use in connecting to the mobile network. This setting must match the plan that the service provider has supplied to you. This is also sometimes known as the APN (Access Point Name).
- **Username** and **Password:** For GSM-based mobile service providers, these settings are the username and password of the mobile connection needed to access the mobile network.
- **Device provisioning state:** For CDMA-based mobile service providers, the text below the **Service Provider** selection list states whether the device has already been provisioned. Clicking the **Provision Device** button launches a wizard for provisioning the device. Mobile device provisioning is described next.

Manuals ID 6-01

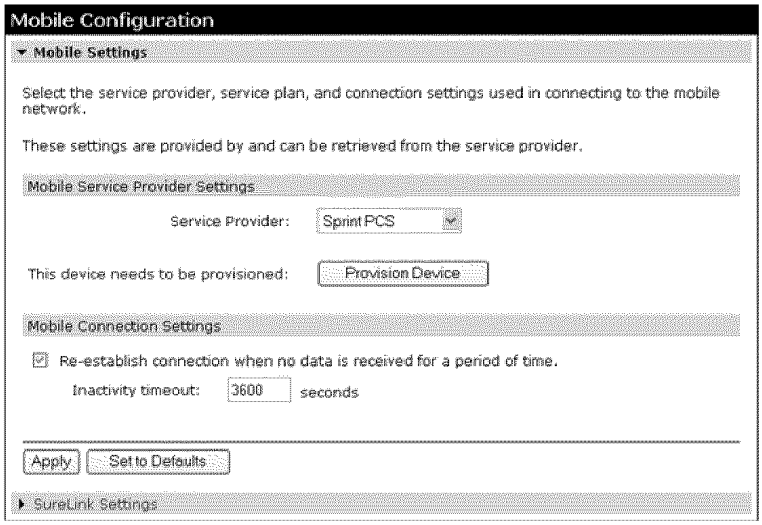
Provision a mobile device

Mobile device provisioning is needed to properly configure the Digi device with the required configuration used to access the mobile network. The device must be provisioned before you will be able to create a data connection to the mobile network.The device only needs to be provisioned once. This type of provisioning applies only to Digi devices that have a CDMA cellular module.

For Digi devices, provisioning is done through the Mobile Device Provisioning Wizard, which is launched from the Mobile Configuration page.

Launch the Mobile Device Provisioning Wizard

Below the **Service Provider** selection list is a line of text that states whether or not the device has already been provisioned or needs to be provisioned. If a device has not yet been provisioned, the Mobile Configuration page displays a message, as shown below. Click the **Provision Device** button to launch the Mobile Device Provisioning Wizard. For example, here is how the **Mobile Settings** page looks when a device has not yet been provisioned.



Automatic versus manual provisioning

There are different types of provisioning methods depending upon your mobile provider. The Mobile Device Provisioning Wizard will provide the appropriate choices based on the mobile provider selected. Two main provisioning methods are:

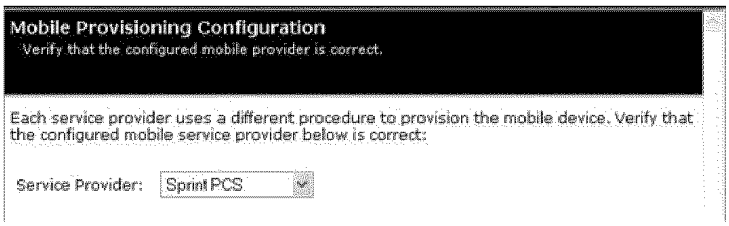
- Automatic Provisioning: Typically, an automatic provisioning process called IOTA (IP-Based Over the Air) is used to provision the device. Note that automatic provisioning requires the modem device to communicate over the mobile network and requires a good signal to ensure proper provisioning.
- Manual Provisioning: Alternatively, a manual provisioning method can be used to manually specify the required fields needed to access the mobile network. The manual provisioning method is an advanced configuration normally used only for custom network access or providers.This method is not available for all mobile providers, and will not be available in the Mobile Device Provisioning Wizard if your mobile provider does not support it.

Example: provision ConnectPort WAN VPN for Sprint™ PCS

The sequence of Mobile Device Provisioning Wizard screens displayed and the settings on them vary by product and mobile service provider. If you used the Digi Device Setup Wizard for initial configuration of your Digi device, and selected a service provider in the wizard, some of the provisioning settings will have already been established.

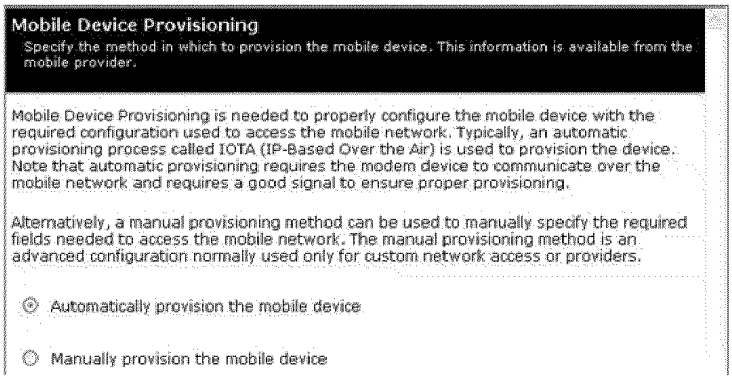
Here is an example of the wizard screens for a ConnectPort WAN VPN using Sprint PCS as the mobile service provider.

1 Select a mobile service provider from the list.



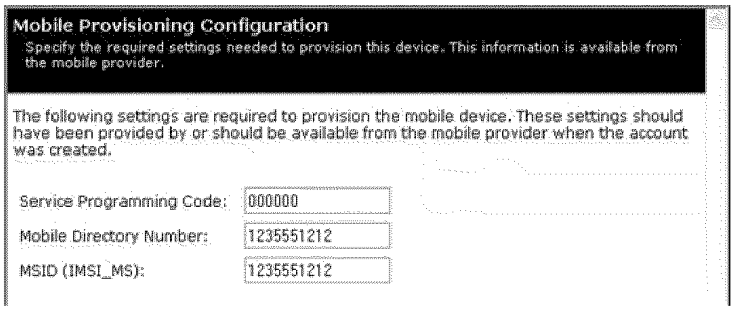
2 Select automatic or manual provisioning.

The main difference between automatic and manual provisioning is that manual provisioning involves entering more information. You will have received all of this information from your mobile service provider during account setup.

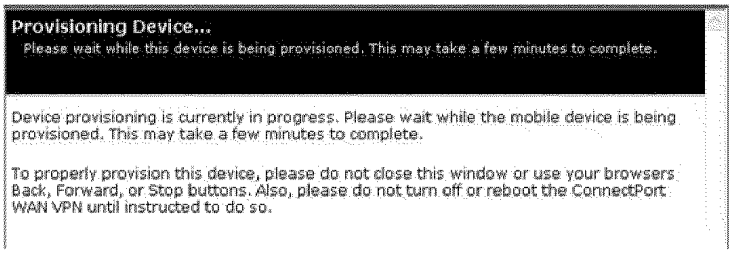


3 Enter device provisioning information provided by your mobile service provider.

If your mobile service provider is Verizon, this screen is not displayed. Instead the settings are already obtained and automatically entered by Verizon's automatic provisioning process.

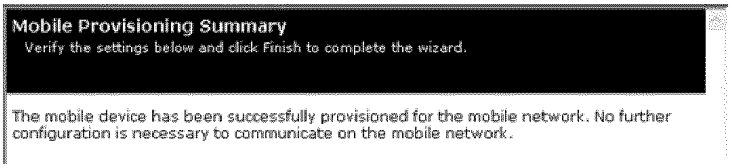


4 Device provisioning in progress...



5 Provisioning complete.

Upon successful completion of provisioning, a screen is displayed stating that the provisioning was successful.Click **Finish.**



6 Click Apply on the Mobile Configuration page to complete the provisioning.

Re-provision a Digi device

Re-provisioning a Digi device simply consists of going through the Mobile Device Provisioning Wizard again.

Manuals ID 6-01

Mobile connection settings

Mobile connection settings configure how the mobile connection is established and maintained.

- **Re-establish connection when no data is received for a period of time:**
  Inactivity timeout: Whether the mobile connection will be disconnected and re-established after no data has been received over the link for the specified amount of time, in seconds.

Digi SureLink™ settings

The Mobile Connection Settings configure Digi SureLink™ settings for a Digi device. SureLink ensures that a Digi device is in a state where it can connect to the mobile network, and they can be used to monitor the integrity of the established mobile connection.

There are two groups of SureLink settings:

- **Hardware Reset Thresholds:** These settings can be configured to clear any error states that were resident in the Digi device's cellular module, so the device can once again connect to the network, if the connection is lost. It does this by first resetting the cellular module after a default or specified number of consecutive failed connection attempts, and then resetting the Digi device after a default or specified number of failed consecutive connection attempts. Each of these connection-failure settings can be disabled as well.
- **Link Integrity Monitoring settings:** These settings can be configured to perform a selected test to examine the functional integrity of the network connection, and take action to recover the connection in the event that it is lost.

Hardware reset thresholds

- **Hard reset the modem module after the following number of consecutive failed connections:** Enables or disables a hard reset of the cellular modem module after the specified number of failed connection attempts.This value can be a number between 1 and 255. The default is 3.
- **Power-cycle the device after the following number of consecutive failed connections:** Enables or disables a power-cycle of the Digi device after the specified number of failed connection attempts. This value can be a number between 1 and 255. The default is 0, or off.

Link integrity monitoring settings

- **Enable Link Integrity Monitoring using the test method selected below:** Enables or disables the link integrity monitoring tests. If this setting is enabled, the other Link Integrity Monitoring settings may be configured and are used to verify the functional integrity of the mobile connection. The default is off (disabled).

  There are three tests available:

  – Ping Test
  – TCP Connection Test
  – DNS Lookup Test

  You can use these tests to demonstrate that two-way communication is working over the mobile connection. Several tests are provided because different mobile networks or firewalls may allow or block Internet packets for various services. Select the appropriate test may be selected according to mobile network constraints and your preferences.

  The link integrity tests are performed only while the mobile connection is established. If the mobile connection is disconnected, the link integrity tests are suspended until the connection is established again.

  For the link integrity tests to provide meaningful results, the remote or target hosts must be accessible over the mobile connection and not through the LAN interface of the device (if it has one). That is, the settings should be configured to guarantee that the mobile connection is actually being tested.

  The link integrity test settings may be modified at any time. The changes are used at the start of the next test interval.

- **Ping Test:** Enables or disables the use of "ping" (ICMP) as a test to verify the integrity of the mobile connection. The test is successful if a valid ping reply is received in response to the ping request sent. The ping test actually sends up to three ping requests, at three second intervals, to test the link. When a valid reply is received, the test completes successfully and immediately. If a reply is received for the first request sent, there is no need to send the other two requests.

  Two destination hosts may be configured for this test. If the first host fails to reply to all three ping requests, the same test is attempted to the second host. If neither host replies to any of the ping requests sent, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.

  – **Primary Address**: First host to test.
  – **Secondary Address**: Second host to test (if the first host fails).

- **TCP Connection Test:** Enables or disables the creation of a new TCP connection as a test to verify the integrity of the mobile connection. The test is successful if a TCP connection is established to a specified remote host and port number. If the remote host actively refuses the connection request, the test is also considered to be successful, since that demonstrates successful two-way communication over the mobile connection. The TCP connection test waits up to 30 seconds for the connection to be established or refused. When the TCP connection is established, the test completes successfully, and the TCP connection is closed immediately.

  Two destination hosts may be configured for this test. If the first host fails to establish (or refuse) the TCP connection, the same test is attempted to the second host. If neither host successfully establishes (or refuses) the TCP connection, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.

  – **TCP Port**: The TCP port number to connect to on the remote host (default 80).
  – **Primary Address**: The address of the first host to test.
  – **Secondary Address**: The address of the second host to test (if the first host fails).

- **DNS Lookup Test:** Enables or disables the use of a Domain Name Server (DNS) lookup as a test to verify the integrity of the mobile connection. The test is successful if a valid reply is received from a DNS server. Typically, this means the hostname is successfully "resolved" to an IP address by a DNS server. But even a reply such as "not found" or "name does not exist" is acceptable as a successful test result, since that demonstrates successful two-way communication over the mobile connection. When a valid reply is received, the test completes successfully and immediately.

  The DNS servers used in this test for the hostname lookup, are the primary and secondary DNS servers obtained from the mobile network when the mobile PPP connection is first established. These addresses can be viewed by going to **Administration > System Information > Mobile**.

  Note that this DNS test is independent of the normal DNS client configuration and lookup cache, which is used for other hostname lookups. This test has been specifically designed to require communication over the mobile connection for each lookup, and to avoid being "short-circuited" by previously cached information. Also, this test does not interfere in any way with the normal DNS client configuration of this device.

  Two hostnames may be configured for this test. If the first hostname fails to get a reply, the same test is attempted for the second hostname. If no reply is received for either hostname, the test fails. The primary and secondary DNS names should be fully qualified domain names. Note that the reverse lookup of an IP address is possible, but that is usually unlikely to succeed in returning a name. Still, such a reverse lookup can be used to demonstrate the integrity of the mobile connection.

  – **Primary DNS Name**: The first hostname to look up.
  – **Secondary DNS Name**: The second hostname to look up (if the first hostname fails).

- **Repeat the selected link integrity test every *N* seconds:** Specifies the interval, in seconds, at which the selected test is initiated (repeated). A new test will be started every ***N*** seconds while the mobile connection is established. This value must be between 10 and 65535. The default is 240.

  If the configured interval is less time than it takes a test to complete, the next test will not be initiated until the previous (current) test has completed.

- **Test only when idle:** if no data is received for the above period of time: Specifies that the test repeat interval (above) is to be used as an idle period interval. That is, initiate the selected link integrity test only after no data has been received for the specified interval of time. This changes the behavior of the test in that the test interval varies according to the presence of other data received from the mobile connection.

  Although using this idle option may result in less data being exchanged over the mobile connection, it also prevents the link integrity tests from running as often to verify the true bi-directional state of that connection.

- **Reset the link after the following number of consecutive link integrity test failures:** Specifies that after the configured number of consecutive link integrity test failures, the mobile connection should be disconnected and reestablished. This value must be between 1 and 255. The default is 3. When the mobile connection is reestablished, the "consecutive failures" counter is reset to zero.

  If the mobile connection is disconnected for any reason (including not as a result of a link integrity test failure), the consecutive failures count is reset to zero when the mobile connection is reestablished.

Status and statistical information for mobile connections

Once the mobile settings have been configured, you can monitor the status of mobile connections by going to **Administration > System Information > Mobile**. See "Mobile information and statistics" on page 163.

From the command line, this mobile information is displayed by issuing **display mobile** and **display pppstats** commands.

Configure Mesh network settings

A Digi ConnectPort X gateway provides a gateway between an Internet Protocol (IP) network and a Mesh network of various ZigBee wireless devices. Typically, these Mesh devices are small sensors and controllers.

On the Mesh network, the ConnectPort X gateway serves as the *coordinator* node. As the coordinator, it is responsible for establishing the operation channel and PAN ID for the entire Mesh network. The ZigBee wireless devices that are discovered and displayed as *routers*.

Mesh/ZigBee network terms

ZigBee stack

ZigBee is a published specification set of high-level communication protocols for use with small, low-power modules. The ZigBee stack provides a layer of network functionality on top of the 802.15.4 specification. For example, the Mesh and routing capabilities available to ZigBee solutions are absent in the 802.15.4 protocol.

ZigBee node types

There are three types of nodes in a Mesh network that uses the ZigBee protocol:

- Coordinator
- Router
- End Device

coordinator

A *coordinator* is node that has the unique function of forming a network. The coordinator is responsible for establishing the operating channel and PAN ID for an entire network. Once established, the coordinator can form a network by allowing routers and end devices to join to it. Once the network is formed, the Coordinator functions like a Router (it can participate in routing packets and be a source or destination for data packets). Characteristics of coordinators include:

- One coordinator per PAN
- Establishes/Organizes PAN
- Can route data packets to/from other nodes
- Can be a data packet source and destination
- Mains-powered

In the web interface, a coordinator is also referred to as a *gateway device*.

router

A *router* is a node that creates/maintains network information and uses this information to determine the best route for a data packet. A router must join a network before it can allow other routers and end devices to join to it. A router can participate in routing packets and is

intended to be a mains-powered node. Characteristics of routers include:

- Several routers can operate in one PAN
- Routers can route data packets to/from other nodes
- Can be a data packet source and destination
- Is mains-powered

end device

End devices have no routing capacity. They must always interact with their parent node (Router or Coordinator) to transmit or receive data. An end device can be a source or destination for data packets but cannot route packets. End devices can be battery-powered and offer low-power operation. Characteristics of end devices include:

- Several end devices can operate in one PAN
- Can be a data packet source and destination
- All messages are relayed through a coordinator or router
- Low power end devices are not supported in this release.

Personal Area Network (PAN)

A data communication network that includes a coordinator and one or more routers/end devices. Net-work formation is governed by network maximum depth, maximum child routers and maximum children end devices. All XBee device adapters are shipped with the same factory default PAN ID. This PAN ID can be changed in the Mesh Network configuration settings in the web interface for the ConnectPort X gateway.

joining

The process of a node becoming part of a ZigBee PAN. A node becomes part of a network by joining to a coordinator or a router (that has previously joined to the network). During the process of joining, the node that allowed joining (the parent) assigns a 16-bit address to the joining node (the child).

network maximum depth

The level of descendents from a coordinator. In a MaxStream PAN, the network maximum depth is 5.

maximum child routers

The maximum number of routers than can join to one node. The maximum number of child routers in a MaxStream PAN is 6.

maximum child end devices

The maximum number of end devices than can join to one node. The maximum number of child end devices in a MaxStream PAN is 14.

network address

The 16-bit address assigned to a node after it has joined to another node.

operating channel

The frequency selected for data communications between nodes. The operating channel is selected by the coordinator on power-up.

energy scan

A scan of RF channels that detects the amount of energy present on the selected channels. The Coordinator uses the energy scan to determine the operating channel.

route request

Broadcast transmission sent by a coordinator or router throughout the network in attempt to establish a route to a destination node.

route reply

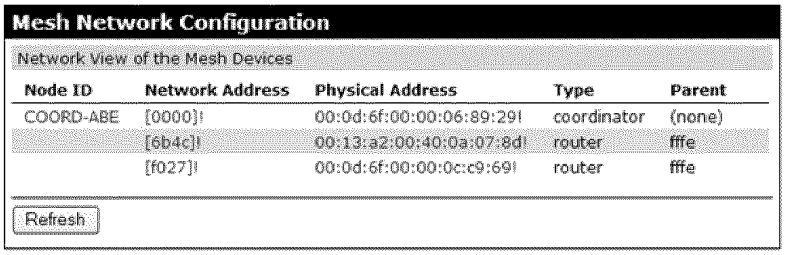
Unicast transmission sent back to the originator of the route request. It is initiated by a node when it receives a route request packet and its address matches the Destination Address in the route request packet.

route discovery

The process of establishing a route to a destination node when one does not exist in the Routing Table. It is based on the AODV (Ad-hoc On-demand Distance Vector routing) protocol.

Mesh Network configuration settings

The Mesh Network Configuration settings (**Configure >** Mesh **Network**) displays a view of Mesh Network components, including the ConnectPort X gateway and any ZigBee nodes that have been discovered by the XBee module in the ConnectPort X gateway. For example:



In the Network View of the Mesh Devices:

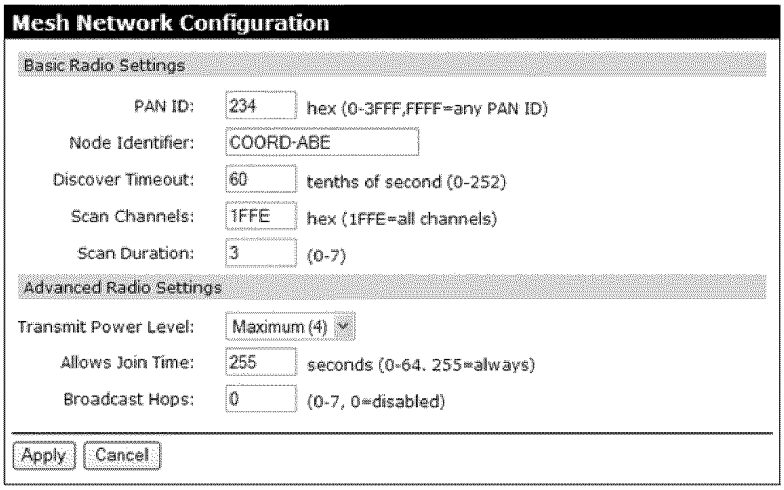
- The ZigBee radio module in the ConnectPort X gateway is listed as the **coordinator**.
- Any ZigBee nodes that are discovered are listed as **routers**.

Configuration settings for the gateway and the ZigBee nodes can be accessed by clicking on the network components displayed in the **Network View of the** Mesh **Devices**.

Manuals ID 6-01

For example, clicking on the coordinator **COORD-ABE** displays the Mesh Network Configuration settings for the XBee radio module in the ConnectPort X gateway. The configuration settings include basic and advanced settings for the XBee radio module.

The configuration settings displayed vary depending on the type of XBee radio installed in your Digi device. The radio settings will include some or all of the settings described in this section.



Basic radio settings

- **PAN ID:** Sets the PAN (Personal Area Network) ID, in hex. This is the preferred PAN ID for the Mesh network. If the configured ID setting is FFFF, the Digi device will select a random PAN ID. Otherwise, the specified ID will be used.

  When a Router or End device searches for a Coordinator on the Mesh network, it joins to a parent that has a matching PAN ID. If that device's configured ID setting is FFFF, the device will join a parent operating on any PAN ID.
- **Node Identifier:** A printable string identifier of this node. This identifier is returned as part of Node Discover command.
- **Discover Timeout:** Sets the amount of time a node will spend discovering other nodes when a Node Join or Node Discover is issued.
- **Scan Channels:** A bit field list of the channels to scan. The Digi device chooses of the channels when starting the network.

  In a Router or End device, the bit field is a list of channels that will be scanned to find a Coordinator/Router to join.
- **Scan Duration:** Sets the scan duration exponent of the Active and Energy Scans (on each channel) that are used to determine an acceptable channel and Pan ID for startup of the Coordinator.

Advanced radio settings

- **Transmit Power Level:** Sets the power level at which the RF module transmits conducted power.

Power Level	Conducted Power in dBm
Lowest (0)	-10 to 10 dBm
Low (1)	-6 to 12 dBm
Medium (2)	-4 to 14 dBm
High (3)	-2 to 16 dBm
Maximum (4)	1 - 18 dBm

- **Allows Join Time:** Determines how long a Coordinator or Router will allow other devices to join it. If set to 255, devices can join at anytime. (This setting is supported on Coordinators and Routers only.)
- **CCA Threshold:** Sets the CCA (Clear Channel Assessment) threshold. Prior to transmitting a packet, a CCA is performed to detect energy on the channel. The packet will not be transmitted if the detected energy is above the CCA threshold.
- **Random Delay Slots:** Sets the minimum value of the back-off exponent in the CSMA-CA algorithm for collision avoidance. If set to zero, collision avoidance is disabled during the first iteration of the algorithm.

- **Broadcast Hops:** Sets the maximum number of hops for each broadcast date transmission. A setting 0 uses the maximum number of hops.

For more information on Mesh networks

The Mesh Network page in System Information (**Administration > System Information >** Mesh **Network**) displays more detailed information about Mesh network devices, including counters related to any applications that are exercising the devices.

Configure serial ports

Use the Serial Port Configuration page to establish a port profile for the serial port of the Digi 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, but not all port profiles are supported in all products. Support of port profiles varies by Digi product. If a profile listed in this description 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.

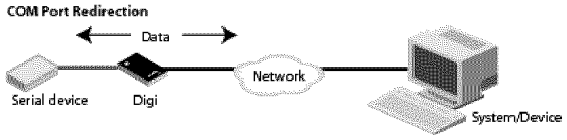
Everything displayed on the Serial Port Configuration screen between **Port Profile Settings** and the links to the **Basic Serial Settings** and **Advanced Serial Settings** depends on the port profile selected.

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 device.

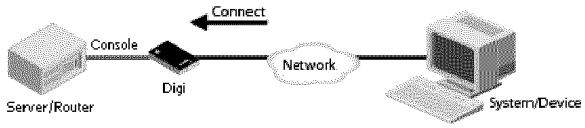


Data is routed to the serial device connected to the Digi device's serial port. The network is transparent to both the application and the serial device.

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 deviceand the RealPort TCP port number 771.

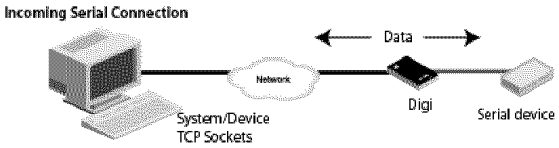
Console Management profile

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 the Digi 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 device.



Automatic TCP connections (autoconnection)

The TCP Client allows the Digi 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 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 device 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 192). No additional configuration is required.

TCP and UDP network port numbering conventions

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

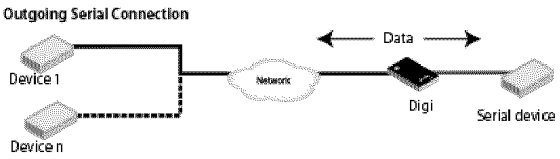
For this connection type...	Use this Port
Telnet to the serial port	2001 (TCP only)
Raw connection to the serial port	2101(TCP and UDP)

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

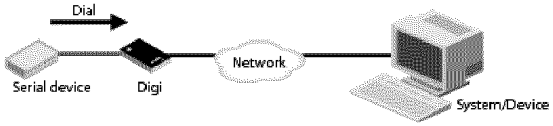
This profile configures each side of the bridge separately. Repeat the configuration for the second Digi device of the bridge, specifying the IP address of the first Digi device.

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 a Digi device to sends and receive 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*.

Dialserv Profile

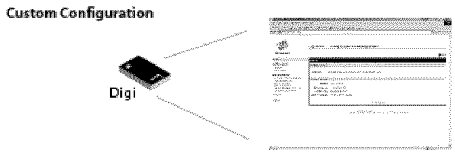
The DialServ Profile allows connecting a DialServ device to the serial port. DialServ simulates a PSTN to a modem and forwards the data to the serial port. The Digi device server sends and receives the data over an IP network.

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.

Manuals ID 6-01

Configure Digi devices



123

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 the Digi device do not need to be changed.

Advanced serial settings

The advanced serial settings 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 theTCP 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 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.

Manuals ID 6-01

- **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 camera settings

ConnectPort X Family products support connecting a WatchPort Camera to one of its USB host ports. One Digi WatchPort V2 USB camera is supported.

Camera settings

These settings configure the operation of the camera and handling of images captured by the camera.

- **Enable Camera:** Enables and disables camera. When disabled, all camera activity stops and all memory used will be freed.
- **Resolution:** The resolution level for images.
- **Frame Delay:** Specify the minimum time (in milliseconds) between frames. The actual delay time between frames will be this number or greater. The camera will automatically increase this value as needed, such as in low light conditions.

  This delay time is the inverse of frames per second. For instance, if you wish to set the camera to process at a maximum of 5 frames per second, the frame delay is set to 200 (1/5 = 0.2 second = 200 ms).
- **Quality:** Choose a quality from 0 to 100. 0 means the lowest quality and smallest image sizes while 100 means the best image quality but largest images.

  Qualities in the range of 30 to 80 are recommended. Quality above 80 will result in much, much larger images than lower qualities, which will result in lower overall performance and increased memory use.
- **Send Images to TCP Server:** Enables sending camera images to a TCP server. The TCP server application must conform to the protocol sent by this device. The protocol is:

  On connect, the TCP client sends a protocol id of four bytes: 0x85ce4a71, followed by a protocol version of 4 bytes: 0x00000010

  After this, images are sent over and over in the form of 4 bytes containing the length of the JPEG image to follow, followed by the JPEG image.
  - **TCP Server:** Name of the server to receive image data.
  - **TCP Port:** TCP port. The default port is 22222.
- **Current Image:** Displays a snapshot of the current camera image. Clicking on the image brings up a new window with the full size image (as configured above).

  If **No Camera Available** is displayed, either the camera is disabled (see above), no camera is attached to the device, or some other problem is causing the camera to not work correctly.

  This current snapshot can be accessed by any web browser directly by using the URL:

  http://device-ip/FS/dev/camera/0
- **Advanced Settings:** All the settings from **Automatic Gain Control** on are advanced camera settings. It is recommended to leave these camera settings to defaults. They can be modified for specific needs by advanced users, but do not need to be modified by most users.

Manuals ID 6-01

Camera operation

Once the camera is connected and configured, the current snapshot image from the camera is available directly from the device at the following URL:

http://device-ip/FS/dev/camera/0

Video from the camera is available by streaming the camera data to a TCP server application, a configured by the **Send Images to TCP Server** configuration settings.

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 includealarms for signal strength and amount of cellular traffic for a given period of time.

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.
- **Send all alarms to the Remote Management server:** enables or disables sending of alarm notifications to the Connectware Manager server.

  Enabling this setting sends all alarm notifications to the Connectware Manager server. Turn this option on if your Digi device is managed by Connectware Manager. Enabling this option is useful because it allows all alarms to be monitored from one location, the Connectware Manager. Enabling this option also allows Digi devices to send alarms to clients that would otherwise be unreachable from the Digi device, either because the Digi device is behind a firewall or not on the same network as the alarm destination.

  Disabling this settings disables sending of alarm notifications to the Connectware Manager server. Leave this option off if you do not manage your devices with Connectware Manager or if you wish to have alarms sent from the device, for example, because an SNMP trap destination is local to the device, not the Connectware Manager server.

  For more information on Connectware Manager, see the *Connectware Manager Getting Started Guide,* and the Connectware Manager online help.
- **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.

Manuals ID 6-01

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 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:** The basis for the alarm.
- **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.

Manuals ID 6-01

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, 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 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.
- **Send alarms based on average RSSI level below threshold for amount of time:** Send alarms based on the average signal strength falling below a specified threshold for a specified amount of time.
  - **RSSI:** The threshold signal strength, measured in dB (typically -120 dB to -40 dB).
  - **Time:** The amount of time, in minutes, that the signal strength falls below the threshold.
- **Send alarms based on cellular data exchanged in an amount of time:**
  - **Data:** The number of bytes of cellular data.
  - **Time:** The number of minutes.
  - **Cell Data Type:** The type of cellular data exchanged: Receive data, Transmit data, or Total data.

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 interface. See "SNMP configuration settings" on page 134. 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 device's name, contact, and location. This device description can be useful for identifying a specific Digi 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 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 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 devices 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 130.
- 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 device knows how to connect to the server.

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

Steps for setting up remote management

Using Connectware Manager as a remote manager of a Digi 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 device. See the *Connectware Manager Operator's Guide's* instructions for adding a device.

   Important: The device ID for the Digi device must be unique. By default, the device ID is created from the MAC address of the device.
3. From the web 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.

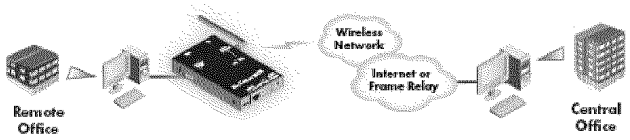
Connection settings

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

To illustrate how both types of connections work, here is a configuration scenario featuring Digi devices communicating over a cellular network with a Connectware Manager server running in the home office.



Addresses for Digi devices can be publicly known, or private and dynamic, or handled through Network Address Translation (NAT). (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. NAT allows a single device, such as a router, to act as an agent between a public network, such as the Internet or a wireless network, and a private, or local, network. This means that only one unique IP address is needed to represent an entire group of computers. Addresses handled through NAT can access the rest of "the world," but "the world" cannot access them.)

In a *client-initiated connection*, the Digi 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 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 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 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 devices have private IP addresses and are behind a NAT.

Last Known Address (LKA)

Manuals ID 6-01

Changes to the IP address for a Digi device present a challenge in server-initiated connections, because the Connectware Manager server needs to locate the Digi 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 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 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 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 device and the Connectware Manager server, and the keep-alive settings of the various interfaces (TCP and HTTP for mobile and 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 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.
- **Mobile Settings:**
  Ethernet Settings: These settings apply to client-initiated management connections over the mobile/cellular and Ethernet networks.
  - **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 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 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 130.

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 Security settings

Security settings involve several areas:

- **User authentication:** whether authentication is required for users accessing the Digi device, and the information required to access it. You can choose to have the user authentication be by username and password or by an SSH public key. Depending on the Digi product, multiple users and their authentication information can be defined. User authentication settings are on the Security settings page.
- **Network Configuration settings to further secure your device:** Digi devices with Cellular capability present additional security considerations, mainly involving securing the border between the Digi device and the cellular network. Several settings on the Network Configuration pages are available to further secure the Digi device.For example, unused network services can be disabled on the **Network Services** page. On the **IP Filtering** page, you can allow access from a specified devices and networks, and drop all other connection attempts.

About user models and user permissions

- In Digi devices that have a one-user model:By default, there is no login prompt.
- The default name for user 1 is **root**. This user is also known as the administrative user.
- User 1 has permissions that enables it to do all commands. Permissions cannot be altered.

Password authentication

By default, there is no password authentication for ConnectPort X Family devices. When accessing the Digi device by opening the web interface or issuing a telnet command, no login prompt is displayed. Enable password authentication

If desired, enable password authentication for the Digi device.

In the web interface:

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

2 On the Security Configuration page, check the **Enable password authentication** check box.

3 Enter the new password in the **New Password** and **Confirm Password** edit boxes.

4 Click **Apply**.

5 A prompt is displayed to immediately log back in to the web interface using the new values.

From the command line:

To enable the login prompt for a device that uses the one-user model, issue a **newpass** command with a password length of one or more characters.

Manuals ID 6-01

Disable password authentication

Password authentication can be disabled as needed.

In the web interface:

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

2 On the **Security 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 interface:

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

2 On the **Security Configuration page**, 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**.

3 A logoff is forced immediately. Log in to the web interface using the new values.

From the command line:

Issue the **newpass** command.

Upload an SSH public key

SSH can be configured to log into to servers without having to provide a password. This is called “public key authentication” and is more secure than using a normal password.

You generate a public/private key using a program called ssh-keygen, and store a copy of the public key on the server(s) that you wish to use for authentication. When you attempt to log in, the server sends you a message encrypted with your public key. Your machine decrypts it and sends back the original message, proving your identity.

To upload an SSH public key:

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

2 On the Security Configuration page, check the Enable SSH public key authentication check box.

3 Type or paste the SSH public key in the edit box.

4 Click **Apply**.

Disable unused and non-secure network services

Depending on your mobile service provider, other users can access your Digi device device over the Internet, through various network services enabled on your Digi device. To further secure the Digi 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 69.

Use IP filtering

You can better restrict your device on the network by only allowing certain devices or networks to connect. This is known as IP filtering or Access Control Lists (ACL). IP filtering configures a Digi device to accept connections from specific and known IP addresses or networks only, and silently drop other connections. Digi devices can be filtered on a single IP address or restricted as a group of devices using a subnet mask that only allows specific networks to access to the device. IP Filtering settings are a part of the Network configuration settings. See "IP filtering settings" on page 74.

Important: Plan and review your IP filtering settings before applying them. Incorrect settings can make the Digi device inaccessible from the network.

Configure applications

Several Digi devices 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**.

Industrial Automation/Modbus Bridge

Industrial Automation is supported in these Digi devices: ConnectPort X2 (non-Python version), and ConnectPort X4.

Digi devices that support Industrial Automation have a set of factory defaults for Industrial Automation/Modbus configurations, listed below, that should be sufficient for most industrial automation uses. Review the factory defaults and decide whether changes are needed. If they are, use the "set ia" command from the command-line interface. Currently, from the web interface, it is only possible to select a different port profile than Industrial Automation, or change the serial port settings, such as baud rate and parity.

Factory defaults for Industrial Automation

Here are the factory default configuration settings for Digi devices that support Industrial Automation:

- By default, serial ports are set to use the Industrial Automation port profile. The Industrial Automation port profile defaults to a Modbus/TCP to RTU Bridge configuration. This default assumes Modbus/RTU slaves with addresses from 1-32 are on the serial port. Slaves with addresses 33-254 (also known as Unit Id or Bridge Index in Modbus/TCP) are Modbus/TCP slaves on the local Ethernet subnet. The slave address (33-254) is used as the last octet of the IP address. A future release will allow complete configuration of the Industrial Automation Profile from the web interface. For now, use the "set ia" command from the command-line interface.
- The serial port settings default to 9600:8,N,1. The baud rate and parity can be changed on the **Basic Serial Settings** tab.
- The IP address is assigned *by DHCP client*. There is no fixed IP address; DHCP client is enabled by default. The WAN IA boots assuming it is DHCP client (WAN/VPN default to fixed IP).
- The internal *DHCP server is disabled***.** This is in contrast to other Digi Cellular Family products, where the DHCP server is enabled by default).
- Serial login (terminal) is disabled. The serial port shall be assigned as a Modbus/RTU slave, thus terminal "login" for configuration is disabled.
- Modbus/TCP Masters incoming on TCP port 502 and UDP port 502.
- Modbus/RTU Masters incoming on TCP port 2101 and UDP port 2101.

  Note This default matches the serial configuration, and so it changes to Modbus/ASCII when serial port is changed to Modbus/ASCII).

- Modbus/RTU serial slave on port 1, settings 9600:8,N,1.
- Incoming Unit Id or Slave Address 0 treated as 1, not broadcast.
- Incoming Unit Id or Slave Address 1 to 32 assumed on serial port.
- Incoming Unit Id or Slave Address 33 to 254 assumed to be Modbus/TCP slaves (servers) on local Ethernet port. Slave Address is used for mast octet of local IP, so if WAN IA has the IP 192.168.2.1, then local slaves assumed to be at 192.168.2.33 to 192.168.2.254.
- Default timeouts:

- Serial or Modbus/TCP slave response in 1 second
- Serial responses with less than 20 msec of inter-byte gap.
- IP requests with less than 30 seconds of inter-byte gap (required to assemble fragmented TCP/IP through cellular link).

Known limitations

- Digi RealPort can be used only if the Modbus Bridge function is disabled. RealPort with Modbus/RTU or ASCII cannot be used to access the Modbus Bridge function.
- The outgoing slave idle time used for remote Modbus IP-based slaves does not always close idle sockets predictably.
- While the Modbus bridge is active, do not attempt to "Port Forward" TCP 502 or UDP 502 to local Modbus/TCP servers while the Modbus Bridge is active. This causes neither function to work. Disable the Modbus Bridge if traditional Router/NAT function for Modbus/TCP port 502 is desired.

Disabling and enabling the Modbus Bridge

To disable the Modbus Bridge, select a different port profile. To enable it, reselect the Industrial Automation profile. Any specialized settings that had been set through "set ia" commands are lost by disabling the Modbus bridge. They must be reconfigured when you reselect the Industrial Automation profile.

More information on Industrial Automation/Modbus

For more information on Industrial Automation, see the "set ia" command description in the *Digi Connect Family Command Reference,* and the application note *Remote Cellular TCP/IP Access to Modbus Ethernet and Serial Devices,* part number 90000773, available on the digi.com Support page at http://www.digi.com/support.

Python® program management

ConnectPort X Family products support loading and running programs written in the Python programming language on ConnectPort X devices.

Python is a dynamic, object-oriented language that can be used for developing a wide range of software applications, from simple programs to more complex embedded applications. It includes extensive libraries and works well with other languages. A true open-source language, Python runs on a wide range of operating systems, such as Windows, Linux/Unix, Mac OS X, OS/2, Amiga, Palm Handhelds, and Nokia mobile phones. Python has also been ported to Java and .NET virtual machines.

Recommended distribution of Python interpreter

The current version of the Python interpreter embedded in Digi devices is 2.4.3. Please use modules known to be compatible with this version of the Python language only.

Additional Python programming resources

The *Digi Python Programming Handbook* introduces the Python programming language and describes Digi's implementation of Python modules.

For additional information on the Python Programming Language, go to http://www.python.org/ and click the **Documentation** link.

Python configuration pages

Selecting **Applications > Python** from the main menu for a ConnectPort X Family device displays the Python Configuration pages. These pages are used to:

- Manage Python program files, including uploading them to Digi devices and deleting them as needed.
- Configure Python programs to execute when the Digi device boots, also known as auto-start programs.

Python files

The Python files page is for uploading Python programs to a Digi device, and managing the uploaded files.

- **Upload Files**: Click Browse to select a file to upload to the Digi device and then click Upload.
- **Manage Files:** Select any files to remove from the Digi device and click **Delete**.

Auto-start settings

The Auto-start settings page configures Python programs to execute when the Digi device boots. Up to four entries can be configured.

- **Enable:** When checked, the program specified in the Auto-start command line field will be run when the device boots.
- **Auto-start command line:** Specify the Python program filename to be executed and any arguments to pass to the program. The syntax is:

  filename [arg1 arg2...]

Manually execute uploaded Python programs

To manually execute an uploaded Python program on a Digi device, access the command line of the device. Then type the command:

python *filename [program args...]*

View and manage executing Python programs

The **who** command can be used to view which Python threads are running.

Configuration through the command line

Configuring a Digi devicethrough 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 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 device. For example:

```
#> telnet 192.3.23.5
```

If security is enabled for the Digi 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 device support of commands

To verify whether a Digi devicesupports 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 device. 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:
access control (IP filtering): limit network access to device	set accesscontrol
alarms	set alarms

Manuals ID 6-01

To configure:	Use this command:
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
IP forwarding	set forward
host name	set host
mobile statistics	display mobile
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
provisioning CDMA cellular modules	display provisioning provision
system-identifying information	set system
serial port options--general	set serial
serial TCP	set tcpserial
RealPort configuration options	set realport
router and Network Address Translation settings	set nat
RTS toggle	set rtstoggle
SNMP	set snmp
Telnet control command: send Telnet control command to last active Telnet session	send

Manuals ID 6-01

To configure:	Use this command:
users and passwords	set user newpass
WPAN (ZigBee/Mesh/802.15.4) network settings	set mesh (See command syntax on page 179.)

Configuration through Simple Network Management Protocol (SNMP)

Configuring Digi devices 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 49, 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 interface instead.

Some elements of SNMP configuration can only be configured from the web interface or command line, such as the setting to send alarms as SNMP traps. In the web 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 130. 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 28 and 48. For information on SNMP as a monitoring interface, see page 185.

Manuals ID 6-01

Configuration through Connectware Manager

Configuring Mesh Networks and Nodes through Connectware Manager

Connectware Manager has several views for configuring and managing Mesh networks:

- The Mesh Networks view
- Node view

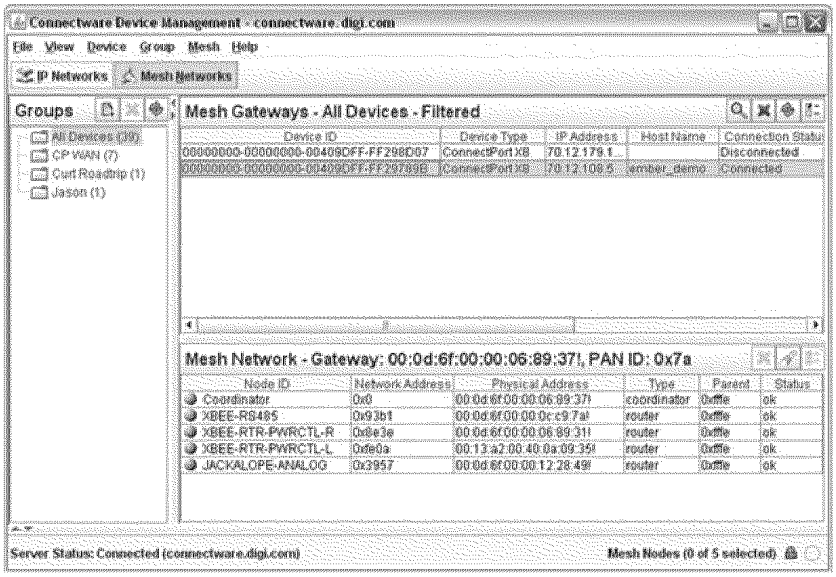
Using Connectware Manager to manage devices in Mesh networks provides several advantages:

- Can run remotely
- Gateway and PAN Management features
- Can view more devices and the entire network, rather than one device at a time
- Caching of previous sets of device configuration settings
- Easier to restructure table

Manuals ID 6-01

Mesh Networks View

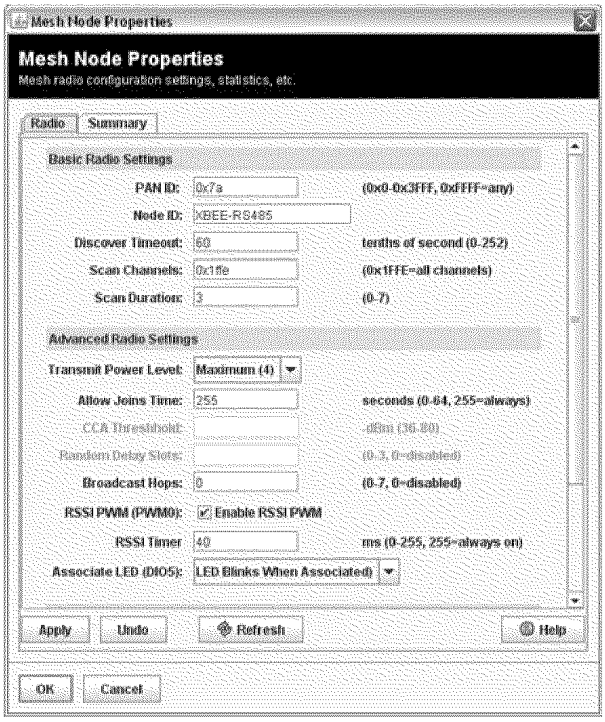
The Mesh **Networks** device management view of Connectware Manager allows for displaying devices within their ZigBee network, including their node ID, the network to which they belong, physical addresses, their role in the ZigBee network (coordinator, router, or end node), and their defined parent in the ZigBee network. Useful information at the bottom of the view includes the state of the battery in the device and the relative signal strength of the radio module in the device.



Manuals ID 6-01

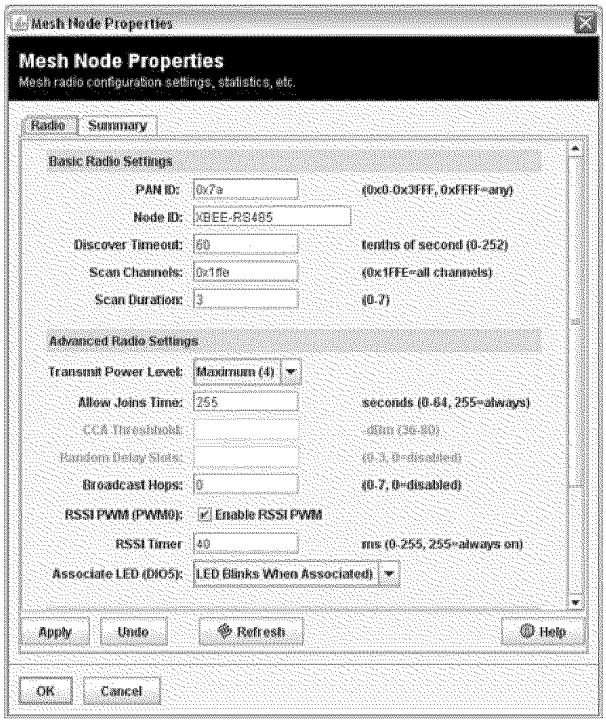
Node View

From the ZigBee Networks view, more detailed views of devices can be accessed. For example, here are the **Radio** and **Summary** tabs of the Mesh **Node Properties** view for a particular ZigBee network node:



Manuals ID 6-01

Configure Digi devices



153

Batch capabilities for configuring multiple devices

For configuring many Digi devicesat 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, "Monitor and manage Digi devices" 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.

Monitor and manage Digi devices

CHAPTER 3

The port, device, system, and network activities of Digi devices can be monitored 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 devices. It covers these topics:

Monitoring capabilities in the web interface

Several device monitoring and connection-management capabilities are available in the web 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, serial port information, network statistics, mobile information and 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.

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.

Manuals ID 6-01

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.

Manuals ID 6-01

Mobile information and statistics

The Mobile information and statistics page displays detailed mobile statistics that may aid in troubleshooting network communication problems with your mobile network. The statistics displayed depend on whether your mobile service provider is GSM- or CDMA-based.

Mobile Connection Statistics

Registration Status

The status of the modem's connection to the cellular network:

- Not Registered: Digi device is not currently searching a new operator to register to.
- Registered: Home Network.
- Not Registered: Digi device is currently searching a new operator to register to.
- Registration Denied.
- Unknown.
- Registered - Roaming.

Cell ID

The modem's identifier in hexadecimal and decimal, for example: "00C3 (195)."

Location Area Code (aka "LAC")

The modem reports this value as a 4-hex-digit string. In the mobile statistics it is displayed both as hex and decimal representations. For example "00C3 (195)."

Signal Strength (RSSI)

The relative signal strength, displayed as signal strength LEDs.

- 0 LEDs: Unacceptable; Signal strength is not known or not detectable.
- 1 LED: Weak.
- 2 LEDs: Moderate.
- 3 LEDs: Good.
- 4: LEDs: Excellent.

Mobile Statistics

Mobile statistics include the interface status, bytes received and sent, baud rate, modem resets, and inactivity timer.

IP Address

The IP address of the PPP connection provided by the mobile service.

Primary DNS Address
Secondary DNS Address

The IP addresses of the DNS nameservers. Name lookups are performed using the nameserver specified on “dns1” first, and if that fails, the nameserver specified on “dns2” is used.

Data Received

Total number of data bytes received.

Data Sent

Total number of data bytes sent.

Idle Resets

The number of times the modem has been reset because no data was received for a period of time.

Inactivity Timer

The time, in seconds, after which if no data has received over the link, the mobile connection will be disconnected and re-established.

Mobile Information

IMSI

International Mobile Subscriber Identifier (IMSI), a unique 15-digit number which designates the subscriber. This ID is the subscriber's code to access the cellular network, and is used by the network for provisioning and to admit the device/user to its provisioned services.

Phone Number

The phone number used to call the modem module. Two numbers are displayed: the Mobile Directory Number (MDN) and the Mobile Identification Number (MIN).

Modem Manufacturer

The manufacturer of the modem module.

Model

The model name of the modem module.

Modem Serial Number

The serial number of the modem module.

Modem Revision

The firmware revision in the modem module.

Other Mobile Information

Depending on your mobile service provider, other mobile information and settings may be provided after the modem revision.

SureLink statistics

Digi SureLink™ provides an “always-on” mobile network connection to ensure that a Digi device is in a state where it can connect to the network.

The statistics displayed for Digi SureLink pertain to the periodic tests, known as Link Integrity Monitoring tests, that are run over the established PPP connection to ensure that end-to-end communication is possible. There are three Link Integrity Monitoring tests available: Ping Test, TCP Connection Test, and DNS Lookup Test. For descriptions of these tests, see "Link integrity monitoring settings" on page 109.

In these SureLink statistics, a “session” is a PPP session. The session statistics are reset to zero at the start of a new PPP connection. The “total” statistics are the accumulated totals for all sessions since the device booted. The “tests” are the SureLink Link Integrity Monitoring tests that have been configured to be run when the mobile network connection is established.

session successes

The number of times a configured test was attempted and succeeded in the current PPP session.

session failures

The number of times a configured test was attempted but failed in the current PPP session.

session consecutive failures

The number of consecutive failures for a test, with no success. When a test is successful, the consecutive failures counter is reset to zero. The consecutive failures counter indicates a device's “progress” toward the configured maximum number of consecutive failures, after which the PPP link is taken down (and restarted).

session bypasses

If a configuration parameter is bad, a test is bypassed rather than considered to have succeeded or failed. This means the test was not run. If the PPP connection goes down while a test is in progress, that test may be classified as bypassed, since it could not be run. (Note that the PPP link may come down for many reasons, independent of SureLink testing.)

total successes

The total number of times a configured test was attempted and succeeded since the Digi device was booted.

total failures

The total number of times a configured test was attempted but failed since the Digi device was booted.

total link down requests

The number of times the SureLink feature has failed consecutively the configured number of failures and, as a result, requested that PPP shut down and restart its connection. This statistic counts such occurrences during the current device boot. SureLink itself does do the PPP stop/start; it sends a message to PPP asking it to do so, owing to a Surelink test failure.

total bypasses

The total test bypasses (see “session bypasses”) since the Digi device was rebooted.

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 Virtual Private Network (VPN) and system connections.

Manage Virtual Private Network (VPN) connections

To monitor a VPN connection from the web interface, select **Management > Connections**. The VPN settings appear. Note that the **Connect** and **Disconnect** functions do not work for a VPN that uses a Pre-Shared Key (PSK).

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 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.

Manuals ID 6-01

Event logging

Management > Event Logging displays the event log for the Digi device. This log records events throughout the Digi device's system, such as starting or resetting the Digi device, configuring features, actions performed by various interfaces and subsystems, starting applications, etc. The event log is always enabled and is not user-configurable. When the Digi device operates in an unexpected manner, the log entries can be set to Digi for analysis by Technical Support and Engineers. The events log cannot be turned off, so that Digi receives an accurate view of all aspects of the operation of the device.

Manage network services

Management > Network Services displays information about active network services. Currently, the only network-service management task possible from this page is managing the DHCP server.

Manage DHCP server operation

DHCP server management operations include:

- View DHCP server status.
- Start/stop/restart the DHCP server.
- View and manage current DHCP leases.

Start, stop, and restart the DHCP server

The DHCP Server Management page shows the current status of the DHCP server. Depending on the current status, there are buttons to start, stop, or restart the DHCP server. Click the appropriate button to perform your request.

Note Stopping, restarting, or rebooting the DHCP server causes all knowledge of the IP address leases to be lost. All leased addresses (except for reservations) will be returned to the available address pool and may be served in a new lease to a DHCP client.

View and manage current DHCP leases

The DHCP server maintains a current list of its leases, reservations and unavailable addresses. The displayed lease list may contain entries that report a variety of status descriptions. The Lease Status types are identified and described below.

Even after a lease has expired or is released by a DHCP client, the associated IP address is not immediately returned to the available address pool. Rather, there is a non-configurable **grace period** during which the lease record is retained by the DHCP server. At the end of that grace period, the lease record is automatically deleted and the associated IP address is returned to the available address pool. Where a grace period is observed, this is indicated in the Lease Status descriptions below.

The grace period is incorporated in the DHCP server to increase the consistency of offering the same IP address to a DHCP client, even if that client is rebooted or off the network for a period of time that does not exceed the grace period.

You can explicitly remove leases from the DHCP server while it is running. To remove a lease, select the checkbox to the left of the lease information in the table of leases, then click the **Remove** button below the lease table. To remove all leases, select the checkbox to the left of the descriptive headings at the top of the table, then click the **Remove** button below the lease table.

Note Removing a lease will cause the associated IP address to be returned immediately to the available address pool. Any IP address in this available address pool may be served in a new lease to a DHCP client.

Static lease reservations will always show in the lease list. These reservation leases may be removed, but a new lease will be created immediately. To disable or permanently remove a reservation, use the DHCP server Settings page in the Network Configuration area.

Lease status types

Descriptions of Lease Status values that are displayed in the lease list follow, including how long a lease table entry will remain in each state. Note that after a lease is deleted, the associated IP address is returned to the available address pool.

Assigned (active)

A lease is currently assigned and active for the given client. The client may renew the lease, in which case the lease remains in this state.

Assigned (expired)

A lease has expired and is no longer active for the given client. A lease in this state will remain for a 4 hour grace period, after which it is deleted. If the same client requests an IP address before the lease is deleted, it will be given the same IP address previously served to it.

Reserved (active)

A lease for an address reservation is currently active for the given client. A reservation lease will remain indefinitely, although the status may alternate between active and inactive.

Reserved (inactive)

A lease for an address reservation is currently inactive for the given client. A reservation lease will remain indefinitely, although the status may alternate between active and inactive.

Reserved (unavail)

A lease for an address reservation was offered to a client, but that client actively declined to use the IP address. Typically this is because the client determined that another host on the same subnetwork is already using that IP address. Upon receiving the client's decline message, the DHCP server will mark the address as unavailable. The lease will remain in this state for 4 hours, after which it is reverts to the Reserved (inactive) status.

Offered (pre-lease)

A lease has been offered to the given client, but that client has not yet requested that the lease be acknowledged. It may be that the client also received an offer from another DHCP server, in which case this offer will expire in approximately 2 minutes. If the client requests this lease before that 2 minute interval elapses, this lease will change status to **Assigned**. If the 2 minute interval expires, the offer record is deleted and the associated IP address is returned immediately to the available address pool.

Released

A lease was previously assigned to the given client, but that client has proactively released it. A lease in this state will remain for a 1 hour grace period, after which it is deleted. If the same client requests an IP address before the lease is deleted, it will be given the same IP address previously served to it.

Unavailable Address

A lease was offered to a client, but that client actively declined to use the IP address. Typically this is because the client determined that another host on the same subnetwork is already using that IP address. Upon receiving the client's decline message, the DHCP server will mark the address as unavailable. The lease will remain in this state for a 4 hour grace period, after which it is deleted. This status may also occur if the DHCP server determines that the IP address is in use before it offers the address to a client (see the DHCP server setting **Check that an IP address is not in use before offering it).**

Manuals ID 6-01

Manage mesh networks

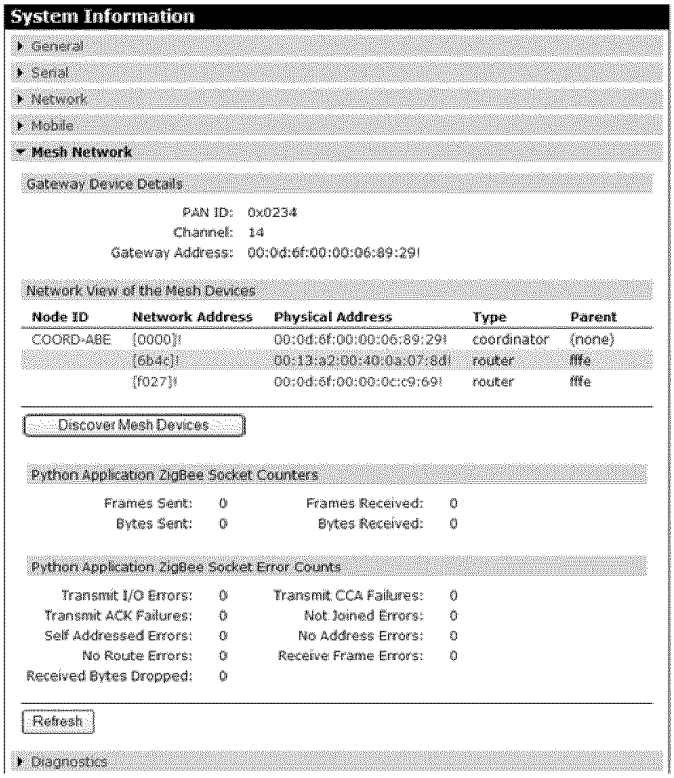
Digi provides several avenues for managing mesh networks and the devices in them:

- From a ConnectPort X device's web interface. This section focuses on this interface.
- From a ConnectPort X device's command-line interface. See "Commands for managing mesh networks and nodes" on page 179.
- From Connectware Manager's Mesh Networks view. See "Monitor/manage mesh networks from Connectware Manager" on page 184.

Manuals ID 6-01

Manage mesh networks from the web interface

To display information about mesh networks and devices within them, select **Administration > System Information > mesh Network**. The mesh Network page is displayed.



Gateway device details

This part of the display shows information about the ConnectPort X gateway and its role as a gateway device in the mesh network. It shows the current PAN ID, Channel, and address in use for the mesh network.

Network view of the mesh devices

This part of the display shows the ConnectPort X gateway and any devices that have joined the mesh network.

Click the **Discover mesh Devices** button to refresh the list of devices that have joined the mesh network. (The discovery operation may take a few seconds.) Click on a device's table entry to view more detailed information of the state of that device.

Python Application ZigBee Socket Counters

This section includes data counters that are specific to ZigBee Sockets implemented using a Python application.

Frames Sent
The total number of transmitted frames.

Frames Received
The total number of received frames.

Bytes Sent
The total number of bytes sent.

Bytes Received
The total number of bytes received.

Python Application ZigBee Socket Error Counts

This section includes error counters that are specific to ZigBee Sockets implemented using a Python application. These values will help determine the quality of data that is being sent or received. Refer to the Troubleshooting information in your User Guide for further help.

Transmit I/O Errors

The total number of transmitted frames which could not be transmitted due to an I/O error.

Transmit CCA Failures

The total number of transmitted frames which could not be transmitted due to a CCA error.

Transmit ACK Failures

The total number of transmitted frames which could not be transmitted due to an ACK error.

Not Joined Errors

The total number of transmitted frames which were attempted to be transmitted to an unjoined node.

Self Addressed Errors

The total number of transmitted frames for which a node attempted to transmit to itself.

No Address Errors

The total number of transmitted frames for which the destination address could not be found.

No Route Errors

The total number of transmitted frames for which a router to the destination could not be found.

Receive Frame Errors

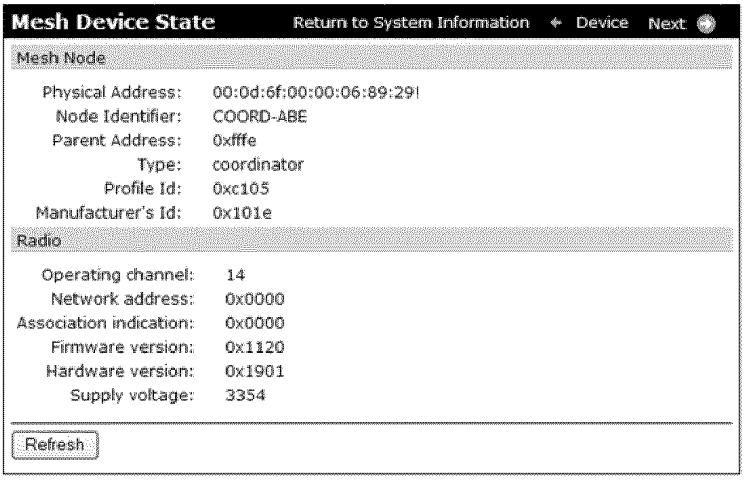
The total number of frames where an error occurred on receive.

Received Bytes Dropped

The total number of bytes dropped due to an exhaustion of internal buffers.

mesh device state pages

Clicking a device in the **Network View of the mesh Devices** displays the **mesh Device State** page for the selected mesh device. This page is used to view more detailed information on the state of the mesh node. The parameters displayed vary based on the capabilities supported by the mesh node's radio module. Here is an example mesh Device State page for the XBee radio module in a ConnectPort X gateway device:



Monitoring capabilities from the command line

There are several commands for monitoring Digi 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

The **display** command 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 interface, command line interface, Point to Point Protocol (PPP), and Ethernet interface, and their status, such as "Closed" or "Connected." (**display netdevice**).
- The event log (**display logging**).
- Memory usage information (**display memory**).
- Serial modem signals. (**display serial**).
- Mobile connection information and statistics (**display mobile**).
- Network Address Translation (NAT) information (**display nat**).
- 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, including results of Link Integrity Monitoring tests by Digi SureLink "**display pppstats**").
- Provisioning information currently in the Digi device device's CDMA module (**display provisioning**)
- Uptime information (**display uptime**).
- Virtual Private Network (VPN) connection information (**display vpn**).

info

The **info** command 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.
- To display mobile statistics, use **display mobile** instead of **info**.

set alarm

The **set alarm** command 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 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.
- **dhcp**: Manages DHCP server operation.
- **exit** and **quit**: These commands terminate a currently active session.
- **vpn**: Manages Virtual Private Network (VPN) connections.
- **who** and **kill**: The **who** command 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.
- **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.

Commands for managing mesh networks and nodes

Several commands are used to configure mesh networks and display information and statistics about the devices in the mesh network: **set mesh**, **display mesh**, and **info zigbee_sockets**.

set mesh

The **set mesh** command configures mesh network settings for a ConnectPort X gateway. Also displays current configuration parameters on the gateway mesh node or of remote nodes in the mesh (specified by the **address** option).

Configure mesh **network settings: command syntax**

```
set mesh [options...] [device_settings...]

options:

    state={off|on}              {Enable mesh gateway}
    address=device address      {Specify device to set}

device_settings:
    pan_id=0x0-0x3fff           {PAN identifier}
    dest_addr=address           {Destination address}
    delay_slots=0-3             {Random delay slots}
    broadcast_hops=0-10         {Broadcast radius}
    scan_channels=0x1-0xffff    {Scan channels, bitfield}
    scan_duration=0-7           {Scan duration, exponent}
    join_time=0-255             {Node join time, sec}
    join_notification=0-2       {Join notification}
    node_id=0-20 chars          {Node identifier}
    discover_timeout=0-252      {Node discovery timeout, x 100 msec}
    aggregation=0-255           {Aggregation route notification, x 10 sec}
    power_level=0-4             {Transmit power level}
    power_mode=0-1              {Power mode}
    cca_threshold=36-80         {CCA threshold, -dBm}
    sleep_period=32-2800        {Cyclic sleep period, x 10 msec}
    device_type=0x0-0xffff      {Device type identifier}
    serial_rate=0-115200        {Serial interface data rate}
    serial_parity=0-4           {Serial interface parity}
    packet_timeout=0-255    {Packetization timeout, chars}
    dio0_config=0-5         {AD0/DIO0 configuration}
    dio1_config=0-5         {AD1/DIO1 configuration}
    dio2_config=0-5         {AD2/DIO2 configuration}
    dio3_config=0-5         {AD3/DIO3 configuration}
    dio4_config=0-5         {DIO4 configuration}
    dio5_config=0-5         {DIO5 configuration}
    dio6_config=0-1         {DIO6 configuration}
    dio7_config=0-7         {DIO7 configuration}
    pwm0_config=0-5         {PWM0 configuration}
    dio11_config=0-5        {DIO11 configuration}
    dio12_config=0-5        {DIO12 configuration}
```

```
rssi_timer=0-255         {RSSI PWM timer, x 100 msec}
pullup_enable=0x0-0x1fff {Pull-up resistor enable, bitfield}
sleep_mode=0-5           {Sleep mode}
sleep_time=0-65535       {Time before sleep, msec}
sleep_count=0-65535      {Peripheral sleep count}
command_timeout=2-655    {Command mode timeout, x 100 msec}
guard_times=2-3300       {Guard times, msec}
command_char=char        {Command sequence character}
```

Display mesh network configuration settings: command syntax

To display the current configuration settings for a mesh network device, use the **set mesh** command. Command syntax is:

```
set mesh [addr=address]
```

display mesh

The **display mesh** command refreshes the display of Mesh network devices, and displays specific information about Mesh network devices.

Command syntax is:

```
display mesh [options...]
options:
          refresh                    {Discover network devices}
          address=device address     {Specify device to display}
```

For example, here are two "display mesh" commands. The first one displays the Mesh network device list. The second displays information about one of the routers in the list.

```
#> display mesh

mesh network device list

PAN ID:           0x007a
Channel:          18
Gateway address:  00:0d:6f:00:00:06:89:37!

Device address           Node Parent Manufacturer Profile Label
------------------------ ---- ------ ------------ ------- -----
COORDINATOR
00:0d:6f:00:00:06:89:37! 0000 fffe   101e         c105    Coordinator

ROUTERS
00:0d:6f:00:00:06:89:31! 8e3e fffe   101e         c105    XBEE-RTR-PWRCTL-R
00:0d:6f:00:00:0c:c9:7a! 93b1 fffe   101e c105    XBEE-RS485
00:13:a2:00:40:0a:09:35! fe0a fffe   101e         c105    XBEE-RTR-PWRCTL-L

END NODES

To display device details:
    display mesh address=(device address)
```

```
#> display mesh address=00:0d:6f:00:00:06:89:31!

Status of device: 00:0d:6f:00:00:06:89:31!

channel          : 18
net_addr         : 0x8e3e
association      : 0x0
firmware_version : 0x1220
hardware_version : 0x1901
supply_voltage   : 3289 (mvolts)
```

info zigbee_sockets

The **info zigbee_sockets** command displays statistics from the ConnectPort X gateway's perspective of what is happening on the ZigBee network. This is essentially data from the MaxStream module's perspective as interpreted by the ZigBee driver in the gateway.

Command syntax is:

```
info zigbee_sockets
```

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, Mesh network overview and detailed information on network nodes.
- Mobile 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.

Manuals ID 6-01

Monitor/manage mesh networks from Connectware Manager

Digi's Connectware Manager provides remote network management of all connected hardware, including devices on the ZigBee network. In contrast to the one-user-to-one device model of other Digi device interfaces, Connectware Manager deploys a one-user-to-many-devices interface model. From Connectware Manager, you can provision and configure network hardware, track device performance, remotely set filters and alarms, monitor connections, reboot devices and reset defaults, and remotely upgrade firmware. ZigBee extensions to Connectware Manager make it a particularly attractive platform for managing ZigBee devices behind the gateway. It displays all nodes on the ZigBee network with the ability to query for node profiles, node descriptors, connected endpoints, radio configuration settings radio statistics, bindings, and more.

Several views in Connectware Manager are used for viewing and configuring ZigBee networks:

- ZigBee Networks View
- Node View

See "Configuring Mesh Networks and Nodes through Connectware Manager" on page 150 for examples of these views.

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.

Manuals ID 6-01

Administration tasks

CHAPTER 4

This chapter discusses the administration tasks that need to be performed on Digi 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 interface
- Administration from the command-line interface
- Administration from Connectware Manager

Administration from the web interface

The Administration section of the web 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 188.
- **Python Program File Management:** For uploading custom programs in the Python programming language to Digi devices and configuring the programs to execute automatically at startup. See "Python® program management" on page 144.
- **X.509 Certificate/Key Management:** For loading and managing X.509 certificates and public/private host key pairs that are public key infrastructure (PKI) based security. See page 189.
- **Backup/Restore:** For backing up or restoring a device's configuration settings. See "Backup/restore device configurations" on page 190.
- **Update Firmware:** For updating firmware, including Boot and POST code. See "Update firmware and Boot/POST Code" on page 191.
- **Factory Default Settings:** For restoring a device to factory default settings. See "Restore a device configuration to factory defaults" on page 192.
- **System Information:** For displaying general system information for the device and device statistics. See "Display system information" on page 193.
- **Reboot:** For rebooting the device. See "Reboot the Digi device" on page 193.

These administrative tasks are organized elsewhere in the web interface:

- Enable and disable network services. See "Network services settings" on page 69.
- Enable password authentication for the Digi device. See "Configure Security settings" on page 140.

File management

The **File Management** page of the web interface uploads custom files to a Digi device, such as the files for a custom applet, or a custom image file of your company logo. 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 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 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 devicefrom 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 192). 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.

X.509 Certificate/Key Management

The X.509 Certificate/Key Management pages are for loading and managing X.509 certificates and public/private host key pairs that are public key infrastructure (PKI) based security. There are several pages for managing several certificate databases:

- The **Certificate Authority (CA) database** is used to load certificate authority digital certificates. A certificate authority (CA) is a trusted third party which issues digital certificates for use by other parties. Digital certificates issued by the CA contain a public key. The certificate also contains information about the individual or organization to which the public key belongs. A CA verifies digital certificate applicants' credentials. The CA certificate allows verification of digital certificates, and the information contained therein, issued by that CA.
- The **Certificate Revocation List (CRL) database** is used to load certificate revocation lists for loaded CAs. A certificate revocation list (CRL) is a file that contains the serial numbers of digital certificates issued by a CA which have been revoked, and should no longer be trusted. Like CAs, CRLs are a vital part of a public key infrastructure (PKI). The digital certifiicate of the corresponding CA must be installed before the CRL can be loaded.
- The **Virtual Private Networking (VPN) Identities database** is used to load host certificates and keys. Identity certificates and keys keys allow for IPSec authentication and secure key exchange with ISAKMP/IKE using RSA or DSA signatures. The VPN identity certificate must be issued by a CA trusted by the peer.
- The **Secure Sockets Layer (SSL) and Transport Layer Security (TLS) databases** are used to load host certificates and keys, as well as peer certificates and revocations.
- The **Secure Shell (SSHv2) Hostkeys database** is used to load host private keys. SSHv2 host keys are used for authentication with SSHv2 clients and secure key exchange. A default 1024-bit DSA key is generated automatically if none exists when the device boots.

Backup/restore device configurations

Once a Digi 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.

In the web interface:

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 firmware and/or boot/POST code for a Digi device 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 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 interface. For details, see "Administration from the command-line interface" on page 194.

Restore a device configuration to factory defaults

Restoring a Digi 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 188 for information on loading and deleting files.

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

Settings cleared and retained during 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 interface

1. Make a backup copy of the configuration using the Backup/Restore operation, described on page 190.
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 interface, the configuration can be restored to factory defaults by using the Reset button.

Display system information

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

From the web interface menu, select **Administration > System Information**. Select **General**, **Serial** or **Network** for the appropriate information. For descriptions of the information displayed on these screens, see page 156.

Reboot the Digi device

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

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

Enable/disable access to network 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 device. In the web interface, enabling and disabling network services is done on the **Network Services** settings page for a Digi device. See "Network services settings" on page 69.

Administration from the command-line interface

Administrative tasks for Digi devices 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 1 Telnet to the Digi device's command line interface using a telnet application or hyperterm. 2 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. 3 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

Manuals ID 6-01

Specifications and certifications

CHAPTER 5

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

Hardware specifications

ConnectPort X2 specifications

Specification		Value
Environmental	Ambient temperature	-40 to 185F (-40 to 85 C)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	-40 to 185F (-40 to 85C)
	Altitude	6560 feet (2000 meters)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263
Power requirements	DC power input	■ 9-30VDC ■ Power consumption: Idle: 0.6 W Max: 1.8 W For ConnectPort X2 XTend/XStream variants: Idle: 0.2 W; Max: 9.9 W ■ Connector: 2.35mm x 5.7mm, locking barrel, center pin positive.
	AC power supply (domestic SKUs)	Can be powered by an external power supply. ■ Certifications: UL /c-UL Listed ITE (LPS) or Class II power supply ■ Input voltage: 120 VAC +/- 10% ■ Input frequency: 60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 500 mA ■ Temperature range: +32 to 104F (0 to 40C). ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.
	AC power supply (international SKUs)	■ Certifications: CE/UL /c-UL Listed ITE or Class II power supply ■ Input voltage: 100 VAC to 240 VAC ■ Input frequency: 50-60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 1.66 A ■ Temperature range: +32 to 104F (0 to 40C). ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.
Dimensions	Length	■ 4.5 in (11.4 cm) ■ For ConnectPort X2 XTend/XStream variants: 6.2 in (15.75 cm)
	Width	2.75 in (7.0 cm)
	Height	1.125 in (2.9 cm)
	Weight	0.44 lb (0.20 kg)

Manuals ID 6-01

ConnectPort X4 product specifications

Specification		Value
Environmental	Ambient temperature	+32 to 104F (0 to +40C)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	-40 to 185F (-40 to 85C)
	Altitude	6560 feet (2000 meters)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263
Power requirements	DC power input	■ Voltage input: 6-30VDC ■ Power consumption: Idle: 1.5W Max: 10.4W ■ Connector: 2.35mm x 5.7mm, locking barrel, center pin positive.
	AC power supply	■ Certifications: CE/UL /c-UL Listed ITE (LPS) or Class II power supply ■ Input voltage: 100 VAC to 240 VAC ■ Input frequency: 50-60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 1.66 A ■ Temperature range: +32 to 104F (0 to 40C) ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.
Dimensions	Length	5.25 in (13.3 cm)
	Width	3.35 in (8.5 cm)
	Depth	0.97 in (2.5 cm)
	Weight	2.60 lb (1.18 kg)

Manuals ID 6-01

ConnectPort X4 NEMA product specifications

Specification		Value
Environmental	Ambient temperature	-40F to 140F (-40C to +60C)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	-40 to 185F (-40 to 85C)
	Altitude	6560 feet (2000 meters)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263
Power requirements	DC power input	■ Voltage input: 6-30VDC ■ Power consumption: Idle: 1.5W Max: 10.4W ■ Connector: 2.35mm x 5.7mm, locking barrel, center pin positive.
	AC power supply	■ Certifications: CE/UL /c-UL Listed ITE (LPS) or Class II power supply ■ Input voltage: 100 VAC to 240 VAC ■ Input frequency: 47-63 Hz ■ Max input watts: 25W max ■ Power: US power cord or European cord option
Dimensions	Length	9.5 in (24.13 cm)
	Width	6.25 in (15.88 cm)
	Depth	3.5 in (8.89 cm)
	Weight	3.2 pounds (1.45 kg)
Mounting orientation (ConnectPort X NEMA only)		The ConnectPort X4 NEMA should be mounted to a flat, secure surface with the cable strain release facing downward.

Manuals ID 6-01

ConnectPort X8 product specifications

Specification		Value
Environmental	Ambient temperature	+32 to 104F (0 to 40C)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	-40 to 185F (-40 to 85C)
	Altitude	6560 feet (2000 meters)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263
Power requirements	DC power input	■ Voltage input: 9-30VDC ■ Power consumption: Idle: 1.2W Max: 3.4W ■ Connector: 2.35mm x 5.7mm, locking barrel, center pin positive.
	AC power supply	■ Certifications: CE/UL /c-UL Listed ITE (LPS) or Class II power supply ■ Input voltage: 100 VAC to 240 VAC ■ Input frequency: 50-60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 1.66 A ■ Temperature range: +32 to 104F (0 to 40C). ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.
Dimensions	Length	7.75 in (19.7 cm)
	Width	4.11 in (10.40 cm)
	Height	1.30 in (3.30 cm)
	Weight	Without a module: 1.40 lb (0.64 kg) With a module: 1.50 lb (0.68 kg)

Manuals ID 6-01

Regulatory information and certifications

FCC certifications and regulatory information (USA only)

FCC Part 15 Class B

These devices comply with the standards cited in this section:

- ConnectPort X2
- ConnectPort X4
- ConnectPort X8

Radio Frequency Interface (RFI) (FCC 15.105)

This device has been tested and found to comply with the limits for Class B digital devices pursuant to Part 15 Subpart B, 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 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.

If the FCC ID is not visible when installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module FCC ID.

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.

Manuals ID 6-01

Declaration of Conformity

(In accordance with FCC Dockets 96-208 and 95-19)

Manufacturer's Name:	Digi International
Corporate Headquarters:	11001 Bren Road East Minnetonka MN 55343
Manufacturing Headquarters:	10000 West 76th Street Eden Prairie MN 55344

Digi International declares, that the product:

Product Name	**Model Number**
ConnectPort X2	50001527-xx 50001531-xx
ConnectPort X4	50001513-xx
ConnectPort X4 NEMA	50001513-xx
ConnectPort X8	50001358-xx

to which this declaration relates, meets the requirements specified by the Federal Communications Commission as detailed in the following specifications:

- Part 15, Subpart B, for Class B equipment
- FCC Docket 96-208 as it applies to Class B personal computers and peripherals

The product listed above has been tested at an External Test Laboratory certified per FCC rules and has been found to meet the FCC, Part 15, Class B, Emission Limits. Documentation is on file and available from the Digi International Homologation Department.

Industry Canada (IC) certifications

This digital apparatus does not exceed the Class B 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 B prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Manuals ID 6-01

Safety statements

5.10 Ignition of Flammable Atmospheres

Warnings for Use of Wireless Devices

Observe all warning notices regarding use of wireless devices.

Potentially Hazardous Atmospheres

Observe restrictions on the use of radio devices in fuel depots, chemical plants, etc. and areas where the air contains chemicals or particles, such as grain, dust, or metal powders, and any other area where you would normally be advised to turn off your vehicle engine.

Safety in Aircraft

Switch off the wireless device when instructed to do so by airport or airline staff. If the device offers a 'flight mode' or similar feature, consult airline staff about its use in flight.

Safety in Hospitals

Wireless devices transmit radio frequency energy and may affect medical electrical equipment. Switch off wireless devices wherever requested to do so in hospitals, clinics, or healthcare facilities. These requests are designed to prevent possible interference with sensitive medical equipment.

Pacemakers

Pacemaker manufacturers recommended that a minimum of 15cm (6 inches) be maintained between a handheld wireless device and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with independent research and recommendations by Wireless Technology Research.

Persons with Pacemakers:

Should ALWAYS keep the device more than 15cm (6 inches) from their pacemaker when turned ON.

Should not carry the device in a breast pocket.

If you have any reason to suspect that the interference is taking place, turn OFF your device.

Class I Division 2, Groups A,B,C,D Hazardous Location (Pending)

ConnectPort X4 NEMA

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D or Non-hazardous locations only.

Warning: Explosion Hazard - Substitution of components may impair suitability for Class I, Division 2.

Manuals ID 6-01

International EMC (Electromagnetic Emissions/Immunity/Safety) standards

This device complies with the requirements of following Electromagnetic Emissions/Immunity/ Safety) standards standards:

Product	Emissions	Immunity	Safety
ConnectPort X2	EN55022 CISPR22 AN/NZS CISPR22 FCC Part 15 Subpart B Class B ICES-003	EN55024	IEC/EN60950-1
ConnectPort X4	EN55022:2006 AS/NZS CISPR 22:2006 ICES-003 FCC Part 15 Subpart B Class B	EN55024:1998+A1:2001+ A2:2003	IEC/EN60950-1 UL 60950-1 CSA C22.2 No. 60950-1-03
ConnectPort X4 NEMA	EN55022:2006 AS/NZS CISPR 22:2006 ICES-003 FCC Part 15 Subpart B Class B	EN55024:1998+A1:2001+ A2:2003; radiated immunity tested to 10V	IEC/EN60950-1 UL 60950-1 outdoor version CSA C22.2 No. 60950-1-03 UL1604, Class 1 Div 2 Haz Loc (pending)
ConnectPort X8	EN55022:1994 +A1:1995+A2:1997 As/NZS CISPR 22:2004 ICES-003 FCC Part 15 Subpart B class B	EN55024:1998+A1:2001+A 2:2003	UL 60950-1 IEC/EN60950-1 CSA C22.2 No. 60950-1-03

Manuals ID 6-01

Troubleshooting

CHAPTER 6

This chapter provides information on resources and processes available for troubleshooting your Digi device.

Troubleshooting Resources

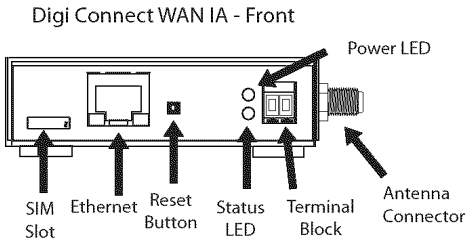
There are several resources available to you for support of your Digi product or resolving configuration difficulties. Try these troubleshooting steps to eliminate your problem. After working through these steps and your problem is not solved, try the resources listed below.

1. Visit our Support knowledge bases at http://www.digi.com/support/knowledgebase.jsp to look for articles related to your situation.
2. Visit our Support Forums at http://www.digi.com/support/forum/ and search for possible posts from other users with similar situations.
3. If the knowledge base or support forums do not have the information you need, fill out an Online Support Request via http://www.digi.com/support/supportrequest.jsp. Creation of a new user account will be required.

Manuals ID 6-01

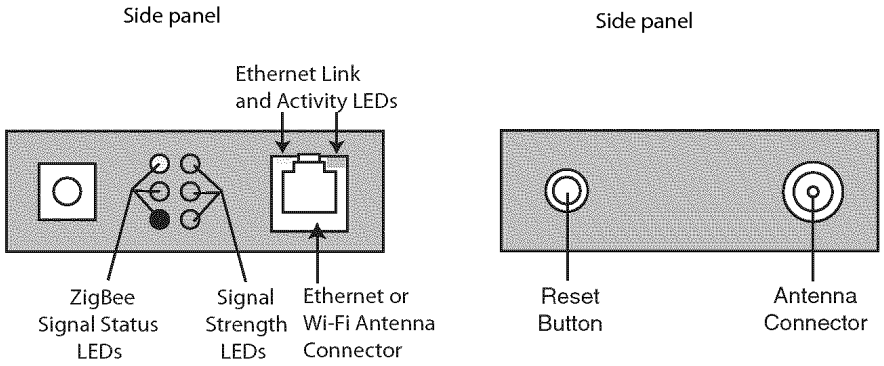
Interpreting the System Status LEDs

Digi devices have several LEDs that indicate system status, link integrity, and link activity. The tables describe the LEDs and the activities they indicate.



Manuals ID 6-01

ConnectPort X2 LEDs and buttons



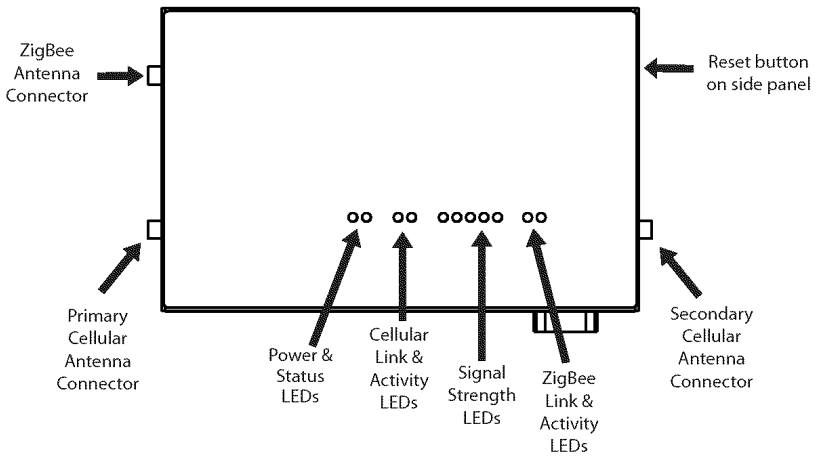
LED/button	Color and Light Pattern	Description
ZigBee Signal Status LEDs		Indicate RF module activity: For more information on this indicator, see the description of the D5 (DIO5 Configuration) parameter in the product manual for the RF module.
	Yellow (top LED)	Serial Data Out (to host)
	Green (middle)	Serial Data In (from host)
	Red (bottom)	Associate/Power Indicator. Indicates both power to the interface board and the network association status for the RF module in the interface board.
	Solid red	RF module powered and not associated to a ZigBee network.
	Blinking red	RF module has associated to a ZigBee network.
Signal Strength LEDs		Indicate the amount of fade margin present in an active wireless link. The fade margin is the difference between the incoming signal strength and the module's receiver sensitivity.
	3 LEDs on	Very Strong Signal (> 30 dB fade margin)
	2 LEDs on	Strong Signal (> 20 dB fade margin)
	1 LED on	Moderate Signal (> 10 dB fade margin)
	0 LED on	Weak Signal (< 10 dB fade margin)

Manuals ID 6-01

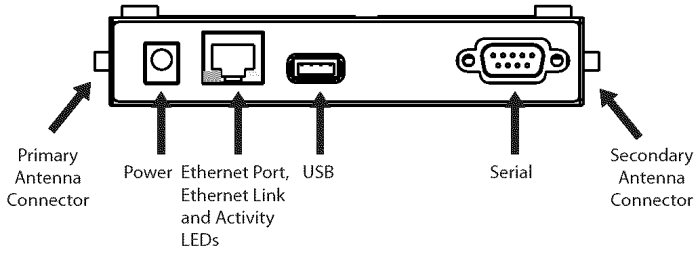
LED/button	Color and Light Pattern	Description
Ethernet Link Status LED	Solid yellow	Ethernet link is up.
Ethernet Activity Status LED	Blinking green	Ethernet traffic is on the link.
Reset button		**Single press**: Performs equivalent of a power-cycle. **Press and hold**: Resets device configuration settings to factory defaults (factory reset).

ConnectPort X4 LEDs and buttons

ConnectPort X4 - Top



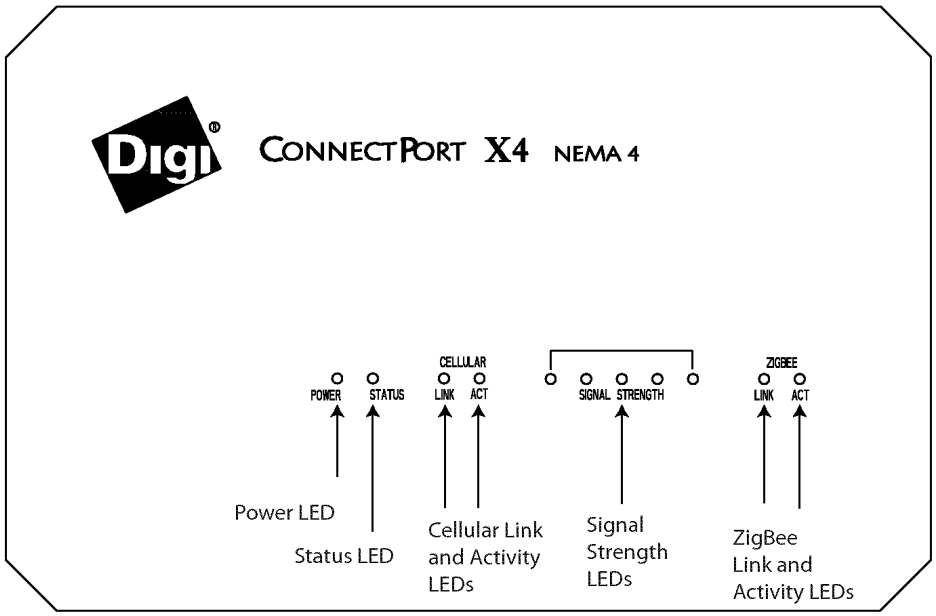
ConnectPort X4 - Front panel



Manuals ID 6-01

ConnectPort X4 NEMA LEDs and buttons

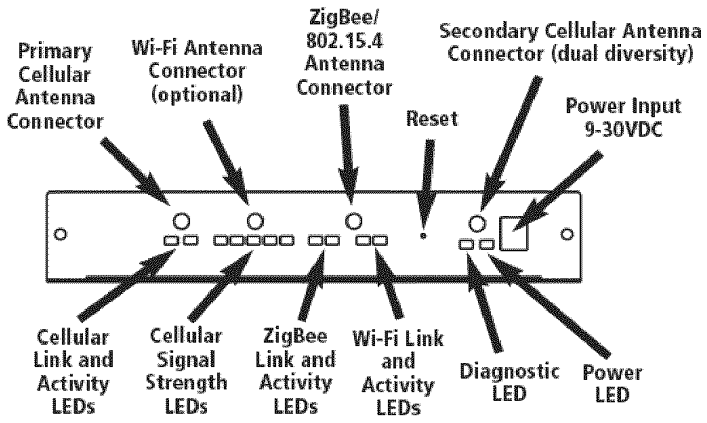
Top Panel



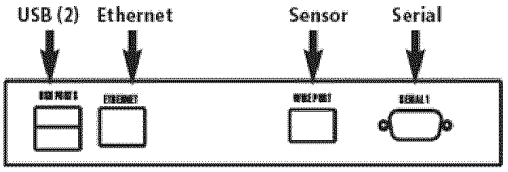
Manuals ID 6-01

ConnectPort X8 LEDs and buttons

- ConnectPort X8 - Front



- ConnectPort X8 - Back



Manuals ID 6-01

LED/button	Color and Light Pattern	Description
Power LED	Blue	Power is applied.
	Not illuminated	No power.
Status LED		Blinks during product initialization and factory reset, using the light patterns below. This LED should never blink during normal operation. If it blinks constantly, contact Digi Technical Support.
	Solid red	Hardware is initializing.
	1-1-1 blinking green	Firmware is initializing.
	1-5-1 blinking green	Device configuration has been restored to its factory defaults.
	Other blinking green	Contact Digi Technical Support.
	Solid green	Device is powered on and ready for operation.
Ethernet Link Status	Solid yellow	Ethernet link is up.
Ethernet Activity Status	Blinking green	Ethernet traffic is on the link.
Cellular Link LED		Cellular link is up.
Cellular Activity LEDs		Cellular traffic is on the link
ZigBee Link and Activity LEDs		Indicate RF module activity: For more information on this indicator, see the description of the D5 (DIO5 Configuration) parameter in the product manual for the RF module.
	Yellow (top LED)	Serial Data Out (to host)
	Green (middle)	Serial Data In (from host)
	Red (bottom)	Associate/Power Indicator. Indicates both power to the interface board and the network association status for the RF module in the interface board.
	Solid red	RF module powered and not associated to a ZigBee network.
	Blinking red	RF module has associated to a ZigBee network.

Manuals ID 6-01

LED/button	Color and Light Pattern	Description
Wi-Fi Link	Green	
Wi-Fi Activity	Yellow	
Signal Strength LEDs	Blue	Indicate the amount of fade margin present in an active wireless link. The fade margin is the difference between the incoming signal strength and the module's receiver sensitivity.
	3 LEDs on	Very Strong Signal (> 30 dB fade margin)
	2 LEDs on	Strong Signal (> 20 dB fade margin)
	1 LED on	Moderate Signal (> 10 dB fade margin)
	0 LED on	Weak Signal (< 10 dB fade margin)
Reset button		**Single press**: Performs equivalent of a power-cycle. **Press and hold**: Resets device configuration settings to factory defaults (factory reset).

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

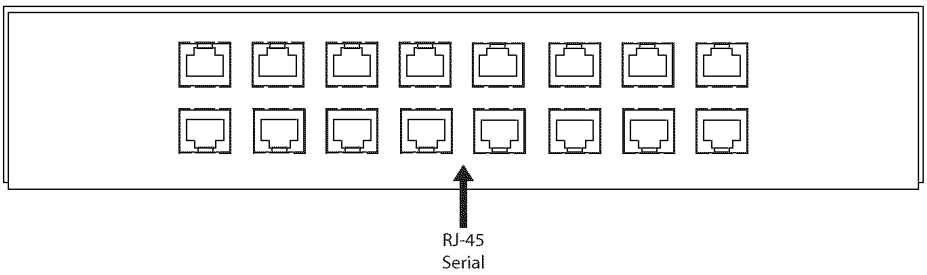
Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Manuals ID 6-01

Digi Connect ES – Back



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 certain data patterns being detected in the data stream and cellular alarms for signal strength and amount of cellular traffic for a given period of time

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.

CDMA

CDMA (Code-Division Multiple Access) protocols are used in wireless communications. CDMA is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHZ bands and through an analog-to digital conversion enhances privacy and makes cloning difficult.

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 management

For Digi 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.

coordinator

In mesh ZigBee networks, a coordinator is node that has the unique function of forming a network. The coordinator is responsible for establishing the operating channel and PAN ID for an entire network. Once established, the coordinator can form a network by allowing routers and end devices to join to it. Once the network is formed, the coordinator functions like a router (it can participate in routing packets and be a source or destination for data packets). Characteristics of coordinators include:

- One Coordinator per PAN
- Establishes/Organizes PAN
- Can route data packets to/from other nodes
- Can be a data packet source and destination
- Mains-powered

In the web interface, a coordinator is also referred to as a *gateway device*.

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 Digi 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.

Encapsulating Security Payload (ESP)

A routing protocol used to route (tunnel) various types of information between networks. See also ESP Passthrough.

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.

end device

In mesh ZigBee networks, end devices are network devices that have no routing capacity. They must always interact with their parent node (router or coordinator) to transmit or receive data. An end device can be a source or destination for data packets but cannot route packets. End devices can be battery-powered and offer low-power operation. Characteristics of end devices include:

- Several end devices can operate in one PAN
- Can be a data packet source and destination
- All messages are relayed through a coordinator or router
- Low power end devices are not supported in this release.

Enhanced Data Rates for Global Evolution (EDGE)

A faster version of the Global System for Mobile (GSM) wireless service, designed to deliver data at rates up to 384 Kbps and enable the delivery of multimedia and other broadband applications to mobile phone and computer users. The EDGE standard is built on the existing GSM standard, using the same time-division multiple access (TDMA) frame structure and existing cell arrangements.

ESP Passthrough

A method of carrying IP packets for a Virtual Private Network (VPN) setup. In ESP Passthrough, inbound IPsec ESP protocol traffic is forwarded from to a VPN device connected to the Digi device's Ethernet port.

Evolution-Data Optimized (EV-DO, EVDO, or 1xEV-DO)

A wireless radio broadband data standard adopted by many CDMA mobile phone service providers. It is standardized by 3GPP2, as part of the CDMA2000 family of standards.

Compared to 1xRTT (CDMA2000 1x) networks, or GPRS and EDGE networks, 1xEV-DO is significantly faster.

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 Packet Radio Service (GPRS)

A packet-based wireless communication service based on Global System for Mobile (GSM) communication that transports data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. Higher data rates allow users more flexibility in the media they transmit.

Generic Routing Encapsulation (GRE)

A routing protocol used to route (tunnel) various types of information between networks. See also GRE Passthrough.

GRE Passthrough

A method of carrying IP packets for a Virtual Private Network (VPN) setup. In GRE Passthrough, inbound IPsec GRE protocol traffic is forwarded from to a VPN device connected to the Digi device's Ethernet port.

Global System for Mobile communication (GSM)

A digital mobile telephone system that digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

GSM

See Global System for Mobile communication.

High Speed Downlink Packet Access (HSDPA)

High Speed Downlink Packet Access. a packet-based data service with data transmission up to 8-10 Mbit/s (and 20 Mbit/s for MIMO systems) over a 5MHz bandwidth in W-CDMA downlink. HSDPA implementations includes Adaptive Modulation and Coding (AMC), Multiple-Input Multiple-Output (MIMO), Hybrid Automatic Request (HARQ), fast scheduling, fast cell search, and advanced receiver design.

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.

IPsec (Internet Protocol Security)

A framework for a set of protocols for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/ Oakley protocol.

Internet Security Association and Key Management Protocol (ISAKMP)

A protocol that defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SAs). SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.

ISAKMP is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP serves as this common framework.

joining

In mesh ZigBee networks, joining is the process of a node becoming part of a ZigBee PAN. A node becomes part of a network by joining to a coordinator or a router (that has previously joined to the network). During the process of joining, the node that allowed joining (the parent) assigns a 16-bit address to the joining node (the child).

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.

Mobile Device Provisioning Wizard

A wizard for provisioning Digi Cellular Family products. Provisioning configures the Digi Cellular Family device with the required configuration used to access the mobile network.

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.

Personal Area Network (PAN)

In mesh ZigBee networks, a PAN is a data communication network that includes a Coordinator and one or more routers/end devices. Network formation is governed by Network Maximum Depth, Maximum Child Routers and Maximum Children End Devices.

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.

provisioning

The process of configuring a mobile (cellular) device with the required configuration used to access the mobile network.

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 login (rlogin)

A remote login to a Digi 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.

router

In mesh ZigBee networks, a router is a node that creates/maintains network information and uses this information to determine the best route for a data packet. A router must join a network before it can allow other routers and end devices to join to it. A router can participate in routing packets and is intended to be a mains-powered node. Characteristics of routers include:

- Several routers can operate in one PAN
- Routers can route data packets to/from other nodes
- Can be a data packet source and destination
- Are mains-powered

RSH

See remote shell.

RSSI

Relative Signal Strength Indicator.

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.

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.

Universal Mobile Telecommunications Service (UMTS)

A third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps) that offers a consistent set of services to mobile computer and phone users no matter where they are located in the world. Based on the Global System for Mobile (GSM) communication standard, UMTS, endorsed by major standards bodies and manufacturers, is the planned standard for mobile users around the world and is at present still being made available. Once UMTS is fully available geographically, computer and phone users can be constantly attached to the Internet as they travel and, as they roam, have the same set of capabilities no matter where they travel to. Users will have access through a combination of terrestrial wireless and satellite transmissions. Until UMTS is fully implemented, users can have multi-mode devices that switch to the currently available technology (such as GSM 900 and 1800) where UMTS is not yet available.

Today's cellular telephone systems are mainly circuit-switched, with connections always dependent on circuit availability. A packet-switched connection, using the Internet Protocol (IP), means that a virtual connection is always available to any other end point in the network. It will also make it possible to provide new services, such as alternative billing methods (pay-per-bit,

pay-per-session, flat rate, asymmetric bandwidth, and others). The higher bandwidth of UMTS also promises new services, such as video conferencing. UMTS promises to realize the Virtual Home Environment (VHE) in which a roaming user can have the same services to which the user is accustomed when at home or in the office, through a combination of transparent terrestrial and satellite connections.

The electromagnetic radiation spectrum for UMTS has been identified as frequency bands 1885-2025 MHz for future IMT-2000 systems, and 1980-2010 MHz and 2170-2200 MHz for the satellite portion of UMTS systems.

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 interface

The web-based interface for configuring, monitoring, and administering Digi devices.

ZigBee

A specification for wireless personal area networks (WPANs) operating at 868 MHz, 902-928 MHz, and 2.4 GHz. A WPAN is a personal area network (a network for interconnecting an individual's devices) in which the device connections are wireless. Using ZigBee, devices in a WPAN can communicate at speeds of up to 250 Kbps while physically separated by distances of up to 50 meters in typical circumstances and greater distances in an ideal environment. ZigBee is based on the 802.15 specification approved by the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA).

ZigBee provides for high data throughput in applications where the duty cycle is low. This makes ZigBee ideal for home, business, and industrial automation where control devices and sensors are commonly used. Such devices operate at low power levels, and this, in conjunction with their low duty cycle (typically 0.1 percent or less), translates into long battery life. Applications well suited to ZigBee include heating, ventilation, and air conditioning (HVAC), lighting systems, intrusion detection, fire sensing, and the detection and notification of unusual occurrences. ZigBee is compatible with most topologies including peer-to-peer, star network,

Manuals ID 6-01

and mesh networks, and can handle up to 255 devices in a single WPAN.

Index

D

T

Manuals ID 6-01

Enclosure

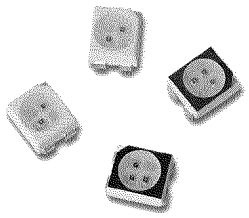
Miscellaneous

Supplement Id	Description
7-05	LED specifications
7-06	Letter of Assurance
7-07	IEC 60950-22 Report

Misc ID 7-05

HSMx-A2xx-xxxxx Bi-Color
HSMx-A3xx-xxxxx Tri-Color
Surface Mount LED Indicators, PLCC-4 SMT LEDs

Data Sheet



Description

This family of SMT LEDs is packaged in the industry standard PLCC-4 package. These SMT LEDs have high reliability performance and are designed to work under a wide range of environmental conditions. This high reliability feature makes them ideally suited to be used under harsh interior automotive as well as interior signs application conditions.

To facilitate easy pick and place assembly, the LEDs are packed in EIA-compliant tape and reel. Every reel will be shipped in single intensity and color bin, except red color to provide close uniformity.

These LEDs are compatible with IR and TTW solder reflow process.

This super wide viewing angle at 120° together with the built in reflector pushing up the intensity of the light output makes these LED suitable to be used in the interior electronics signs. The flat top emitting surface makes it easy for these LEDs to mate with light pipes. This is suitable for general backlighting in automotive interior, office equipment, industrial equipment, and home appliances.

Features

- Industry Standard PLCC-4 package (Plastic Leaded Chip Carrier)
- High reliability LED package
- High brightness using AlInGaP and InGaN dice technologies
- Available in full selection of colors
- Super wide viewing angle at 120°
- Available in 8 mm carrier tape on 7-inch reel
- Compatible with IR soldering process

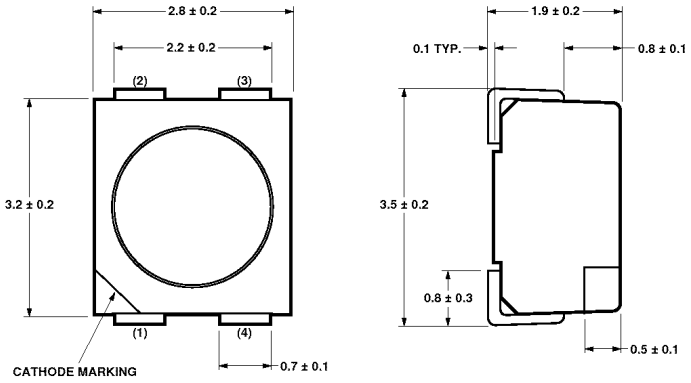
Applications

- Electronic signs and signals
  - Interior full color sign
  - Variable message sign
- Interior automotive
  - Instrument cluster backlighting
  - Central console backlighting
  - Cabin backlighting
- Office automation, home appliances, industrial equipment
  - Front panel backlighting
  - Display backlighting

CAUTION: HSMF-Axxx-xxxxx LEDs are Class 2 ESD sensitive. Please observe appropriate precautions during handling and processing. Refer to Avago Application Note AN-1142 for additional details.

Misc ID 7-05

Package Dimensions



NOTE:
1. ALL DIMENSIONS IN mm.

Tri Color
1 Cathode (Color 1)
2 Common Anode
3 Cathode (Color 3)
4 Cathode (Color 2)
Bi Color
1 Cathode (Color 1)
2 Anode (Color 1)
3 Cathode (Color 2)
4 Anode (Color 2)

Device Selection Guide

Bi Color

Part Number	Color 1	Color 2
HSMF-A201- xxxxx	GaP Red	GaP Yellow Green
HSMF-A202- xxxxx	GaP Red	GaP Yellow
HSMF-A203- xxxxx	GaP Red	GaP Emerald Green
HSMF-A204- xxxxx	GaP Orange	GaP Yellow Green
HSMF-A205- xxxxx	GaP Orange	GaP Emerald Green
HSMF-A206- xxxxx	GaP Yellow	GaP Yellow Green
HSMF-A211- xxxxx	AlGaAs Red	GaP Yellow Green
HSMF-A212- xxxxx	AlGaAs Red	GaP Yellow
HSMF-A222- xxxxx	AlInGaP Red	AlInGaP Amber
HSMF-A227- xxxxx	AlInGaP Red	GaN Blue
HSMF-A228- xxxxx	AlInGaP Amber	GaN Blue
HSMF-A226- xxxxx	AlInGaP Amber	AlInGaP Yellow Green

Misc ID 7-05

	Color 1			Color 2		
Part Number	Min. Iv @ 20 mA Bin ID	(mcd)	Typical Iv @ 20 mA (mcd)	Min. Iv @ 20 mA Bin ID	(mcd)	Typical Iv @ 20 mA (mcd)
HSMF-A201-A00J1	K2	8.0	16.0	L1	10.0	20.0
HSMF-A202-A00J1	K2	8.0	16.0	K1	6.3	12.0
HSMF-A203-A00J1	K2	8.0	16.0	J1	4.0	8.0
HSMF-A204-A00J1	K2	8.0	16.0	L1	10.0	20.0
HSMF-A205-A00J1	K2	8.0	16.0	J1	4.0	8.0
HSMF-A206-A00J1	K2	8.0	16.0	L1	10.0	20.0
HSMF-A211-A00J1	L2	12.5	25.0	L1	10.0	20.0
HSMF-A212-A00J1	L2	12.5	25.0	K1	6.3	12.0
HSMF-A222-A00J1	P1	40.0	80.0	P1	40.0	80.0
HSMF-A227-A00J1	P1	40.0	80.0	J2	5.0	10.0
HSMF-A228-A00J1	P1	40.0	80.0	J2	5.0	10.0
HSMF-A226-A00J1	P2	49.0	100.0	M2	20.0	60.0

Note:
1. The luminous intensity Iv, is measured at the mechanical axis of the lamp package. The actual peak of the spatial radiation pattern may not be aligned with this axis.

Tri Color

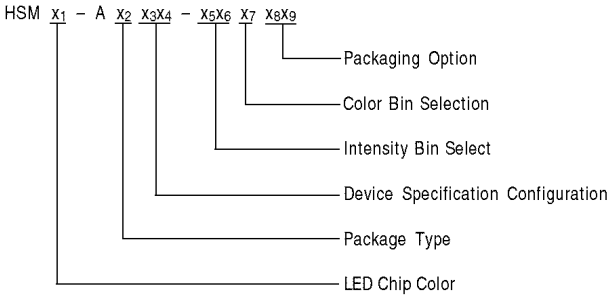
Part Number	Color 1	Color 2	Color 3
HSMF-A301-xxxxx	GaP Red	GaP Yellow Green	GaN Blue
HSMF-A331-xxxxx	AlInGaP Red	InGaN Green	GaN Blue
HSMF-A332-xxxxx	AlInGaP Red Orange	InGaN Green	GaN Blue
HSMF-A341-xxxxx	AlInGaP Red	InGaN Green	InGaN Blue
HSMF-A342-xxxxx	AlInGaP Red Orange	InGaN Green	InGaN Blue

	Color 1			Color 2			Color 3		
Part Number	Min. Iv @ 20 mA Bin ID	(mcd)	Typical Iv @ 20 mA (mcd)	Min. Iv @ 20 mA Bin ID	(mcd)	Typical Iv @ 20 mA (mcd)	Min. Iv @ 20 mA Bin ID	(mcd)	Typical Iv @ 20 mA (mcd)
HSMF-A301-A00J1	K2	8.0	13.0	L2	12.5	20.0	K2	8.0	10.0
HSMF-A331-A00J1	P1	40.0	80.0	R1	99.0	160.0	K2	8.0	10.0
HSMF-A332-A00J1	P1	40.0	80.0	R1	99.0	160.0	K2	8.0	10.0
HSMF-A341-A00J1	P1	40.0	80.0	R1	99.0	160.0	N1	25.0	40.0
HSMF-A342-A00J1	P1	40.0	80.0	R1	99.0	160.0	N1	25.0	40.0

Note:
1. The luminous intensity Iv, is measured at the mechanical axis of the lamp package. The actual peak of the spatial radiation pattern may not be aligned with this axis.

Misc ID 7-05

Part Numbering System



Absolute Maximum Ratings (T_A = 25°C)

Parameters	GaP	AlGaAs	AlInGaP		GaN/ InGaN
			Red, Amber	Yellow Green	
DC Forward Current[1]	30 mA	30 mA	30 mA [3,4]	20 mA [4]	20 mA
Peak Forward Current[2]	100 mA	100 mA	100 mA	100 mA	100 mA
Power Dissipation	78 mW	78 mW	72 mW	48 mW	120 mW
Reverse Voltage	5 V				
Junction Temperature	110°C				
Operating Temperature	–55°C to +100°C				
Storage Temperature	–55°C to +100°C				

Notes:
1. Derate linearly as shown in figure 4.
2. Duty factor = 10%, Frequency = 1kHz.
3. Drive Current between 10 mA and 30 mA are recommended for best long term performance.
4. Operation at current below 5 mA is not recommended.

Misc ID 7-05

Optical Characteristics (T_A = 25°C)

Color	Peak Wavelength λ_{PEAK} (nm) Typ.	Dominant Wavelength λ_D (nm)[1] Typ.	Viewing Angle $2\theta_{1/2}$ (Degrees)[2] Typ.	Luminous Efficacy η_v (lm/ W)[3] Typ.	Luminous Intensity/ Total Flux I_V (mcd) / Φ_V (mlm) Typ.
GaP Red	635	626	120	120	0.45
AlGaAs Red	645	637	120	63	0.45
AlInGaP Red	635	626	120	150	0.45
AlInGaP Red Orange	621	615	120	240	0.45
GaP Orange	600	602	120	380	0.45
AlInGaP Amber	592	590	120	480	0.45
GaP Yellow	583	585	120	580	0.45
AlInGaP Amber	592	590	120	480	0.45
GaP Yellow Green	565	569	120	590	0.45
GaP Emerald Green	558	560	120	650	0.45
InGaN Green	523	525	120	500	0.45
InGaN Blue	468	470	120	75	0.45
GaN Blue	428	462	120	65	0.45
AlInGaP Yellow Green	575	571	120	620	0.45

Notes:

1. The dominant wavelength, λ_D, is derived from the CIE Chromaticity Diagram and represents the color of the device.
2. $\theta_{1/2}$ is the off-axis angle where the luminous intensity is 1/ 2 the peak intensity.
3. Radiant intensity, I_e in watts/ steradian, may be calculated from the equation $I_e = I_v / \eta_v$, where I_v is the luminous intensity in candelas and η_v is the luminous efficacy in lumens/ watt.

Electrical Characteristics (T_A = 25°C)

Dice Technology	Forward Voltage V_F [Volts] @I_F = 20mA Typ.	Max.	Reverse Voltage V_R @ 100 µA Min.	Reverse Voltage V_R @ 10 µA Min.
GaP	2.2	2.6	5	-
AS AlGaAs	1.9	2.6	5	-
AlInGaP	1.7	2.1	5	-
GaN Blue	3.9	4.3	-	5
InGaN	3.4	4.05	-	5

Misc ID 7-05

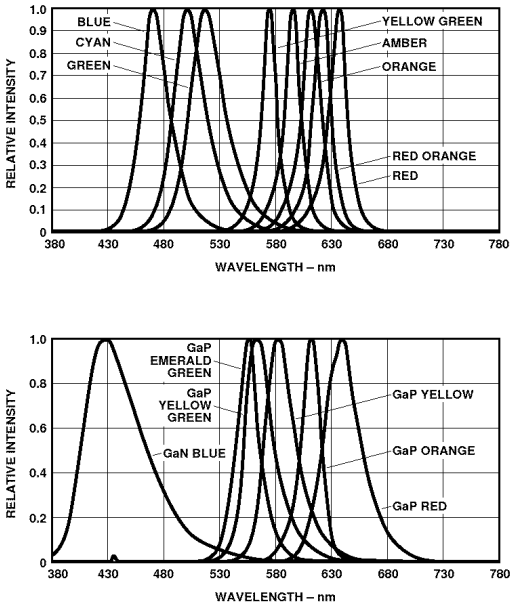


Figure 1. Relative intensity vs. wavelength.

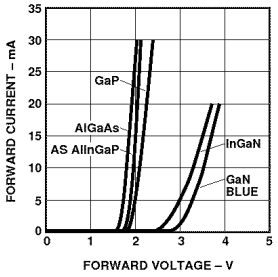


Figure 2. Forward current vs. forward voltage.

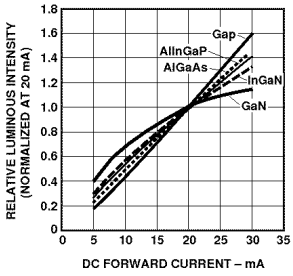


Figure 3. Relative intensity vs. forward voltage.

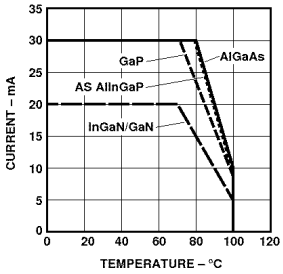


Figure 4a. Maximum forward current vs. ambient temperature. Derated based on $T_J MAX = 110°C$, $R\theta_{JA} = 500°C/W$ (1 chip on).

Misc ID 7-05

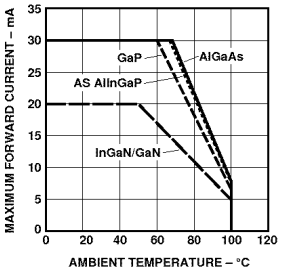


Figure 4b. Maximum forward current vs. ambient temperature. Derated based on $T_J MAX$ = 110°C, $R\theta_{JA}$ = 700°C/ W (3 chip on).

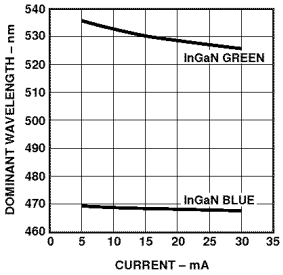


Figure 5. Dominant wavelength vs. forward current – InGaN.

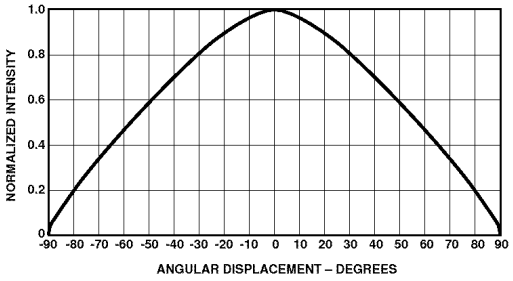


Figure 6. Radiation pattern.

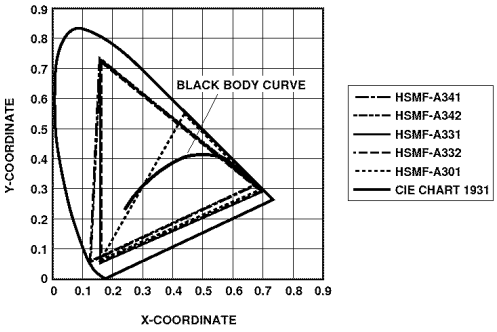


Figure 7. Chromaticity diagram for Tricolor.

Misc ID 7-05

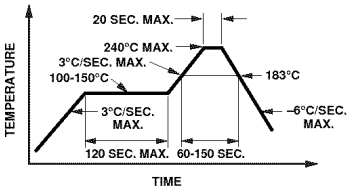


Figure 8a. Recommended SnPb reflow soldering profile.

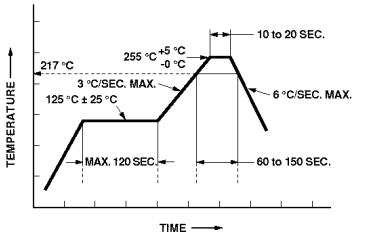


Figure 8b. Recommended Pb-free reflow soldering profile.

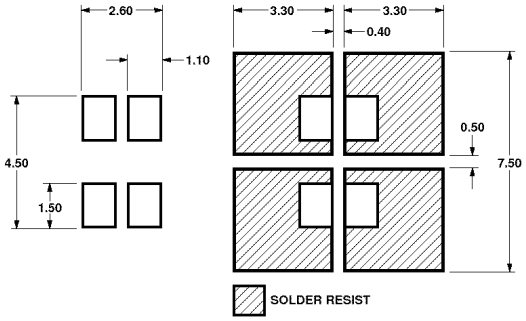


Figure 9. Recommended soldering pad pattern.

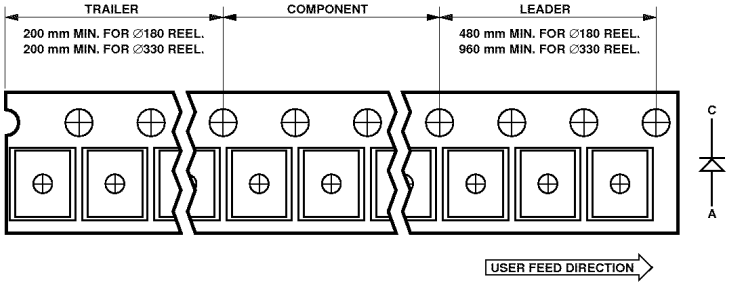


Figure 10. Tape leader and trailer dimension.

Misc ID 7-05

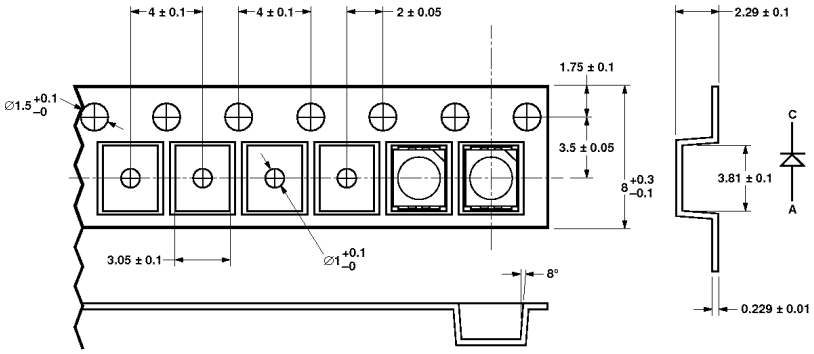


Figure 11. Tape leader and trailer dimension.

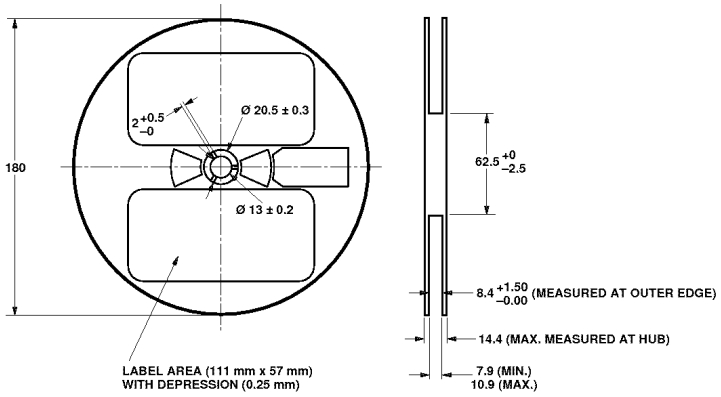


Figure 12. Reel dimension.

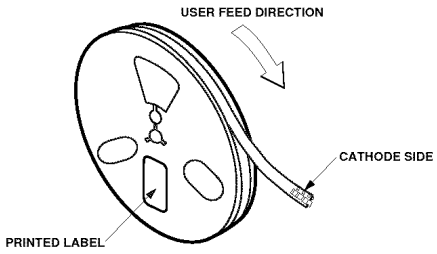


Figure 13. Reeling Orientation.

Storage Condition: 5 to 30°C @ 60% RH max.

Baking is required under the condition:

a) the humidity indicator card becoming pink color
b) the pack has been opened for more than 4 weeks

Baking recommended condition: 60 ± 5°C for 20 hours.

This product is qualified as Moisture Sensitive JEDEC Level 2A.

Misc ID 7-05

Iv Bin Select (X_5X_6)
Individual reel will contain parts from 1 half bin only.

X_5	Min. Iv Bin Selection	
For HSMF-A201-xxxxx HSMF-A204-xxxxx HSMF-A206-xxxxx		
	Minimum Intensity Bin	
	Color 1 (Red/ Yellow/ Orange)	Color 2 (Green)
A	K2	L1
B	K2	L2
C	K2	M1
D	K2	M2
E	K2	N1
F	L1	L1
G	L1	L2
H	L1	M1
J	L1	M2
K	L1	N1
L	L2	L1
M	L2	L2
N	L2	M1
P	L2	M2
Q	L2	N1
R	M1	L1
S	M1	L2
T	M1	M1
U	M1	M2
V	M1	N1
W	M2	L1
X	M2	L2
Y	M2	M1
Z	M2	M2
1	M2	N1

For HSMF-A202-xxxxx		
	Minimum Intensity Bin	
	Color 1 (Red)	Color 2 (Yellow)
A	K2	K1
B	K2	K2
C	K2	L1
D	K2	L2
E	K2	M1
F	L1	K1
G	L1	K2
H	L1	L1
J	L1	L2
K	L1	M1
L	L2	K1
M	L2	K2
N	L2	L1
P	L2	L2
Q	L2	M1
R	M1	K1
S	M1	K2
T	M1	L1
U	M1	L2
V	M1	M1
W	M2	K1
X	M2	K2
Y	M2	L1
Z	M2	L2
1	M2	M1

For HSMF-A203-xxxxx HSMF-A205-xxxxx		
	Minimum Intensity Bin	
	Color 1 (Red/ Orange)	Color 2 (Green)
A	K2	J1
B	K2	J2
C	K2	K1
D	K2	K2
E	K2	L1
F	L1	J1
G	L1	J2
H	L1	K1
J	L1	K2
K	L1	L1
L	L2	J1
M	L2	J2
N	L2	K1
P	L2	K2
Q	L2	L1
R	M1	J1
S	M1	J2
T	M1	K1
U	M1	K2
V	M1	L1
W	M2	J1
X	M2	J2
Y	M2	K1
Z	M2	K2
1	M2	L1

Misc ID 7-05

For HSMF-A211-xxxxx		
	Minimum Intensity Bin	
	Color 1 (Red)	Color 2 (Green)
A	L2	L1
B	L2	L2
C	L2	M1
D	L2	M2
E	L2	N1
F	M1	L1
G	M1	L2
H	M1	M1
J	M1	M2
K	M1	N1
L	M2	L1
M	M2	L2
N	M2	M1
P	M2	M2
Q	M2	N1
R	N1	L1
S	N1	L2
T	N1	M1
U	N1	M2
V	N1	N1
W	N2	L1
X	N2	L2
Y	N2	M1
Z	N2	M2
1	N2	N1

Note: 0 represents no maximum bin limit.

For HSMF-A212-xxxxx		
	Minimum Intensity Bin	
	Color 1 (Red)	Color 2 (Yellow)
A	L2	K1
B	L2	K2
C	L2	L1
D	L2	L2
E	L2	M1
F	M1	K1
G	M1	K2
H	M1	L1
J	M1	L2
K	M1	M1
L	M2	K1
M	M2	K2
N	M2	L1
P	M2	L2
Q	M2	M1
R	N1	K1
S	N1	K2
T	N1	L1
U	N1	L2
V	N1	M1
W	N2	K1
X	N2	K2
Y	N2	L1
Z	N2	L2
1	N2	M1

For HSMF-A222-xxxxx		
	Minimum Intensity Bin	
	Color 1 (Red)	Color 2 (Amber)
A	P1	P1
B	P1	P2
C	P1	Q1
D	P1	Q2
E	P1	R1
F	P2	P1
G	P2	P2
H	P2	Q1
J	P2	Q2
K	P2	R1
L	Q1	P1
M	Q1	P2
N	Q1	Q1
P	Q1	Q2
Q	Q1	R1
R	Q2	P1
S	Q2	P2
T	Q2	Q1
U	Q2	Q2
V	Q2	R1
W	R1	P1
X	R1	P2
Y	R1	Q1
Z	R1	Q2
1	R1	R1
2	R2	P1
3	R2	P2
4	R2	Q1
5	R2	Q2
6	R2	R1

Misc ID 7-05

For
HSMF-A227-xxxxx
HSMF-A228-xxxxx

	Minimum Intensity Bin	
	Color 1 (Red/ Amber)	Color 2 (Blue)
A	P1	J2
B	P1	K1
C	P1	K2
D	P1	L1
E	P1	L2
F	P2	J2
G	P2	K1
H	P2	K2
J	P2	L1
K	P2	L2
L	Q1	J2
M	Q1	K1
N	Q1	K2
P	Q1	L1
Q	Q1	L2
R	Q2	J2
S	Q2	K1
T	Q2	K2
U	Q2	L1
V	Q2	L2
W	R1	J2
X	R1	K1
Y	R1	K2
Z	R1	L1
1	R1	L2
2	R2	J2
3	R2	K1
4	R2	K2
5	R2	L1
6	R2	L2

For
HSMF-A331-xxxxx
HSMF-A332-xxxxx

	Minimum Intensity Bin		
	Color 1 (Red/ Red Orange)	Color 2 (Green)	Color 3 (Blue)
A	P1	R1	K2
B	P1	R1	L1
C	P1	R1	L2
D	P1	R2	K2
E	P1	R2	L1
F	P1	R2	L2
G	P1	S1	K2
H	P1	S1	L1
J	P1	S1	L2
K	P2	R1	K2
L	P2	R1	L1
M	P2	R1	L2
N	P2	R2	K2
P	P2	R2	L1
Q	P2	R2	L2
R	P2	S1	K2
S	P2	S1	L1
T	P2	S1	L2
U	Q1	R1	K2
V	Q1	R1	L1
W	Q1	R1	L2
X	Q1	R2	K2
Y	Q1	R2	L1
Z	Q1	R2	L2
1	Q1	S1	K2
2	Q1	S1	L1
3	Q1	S1	L2
4	Q2	R1	K2
5	Q2	R1	L1
6	Q2	R1	L2
7	Q2	R2	K2
8	Q2	R2	L1
9	Q2	R2	L2

For
HSMF-A341-xxxxx
HSMF-A342-xxxxx

	Minimum Intensity Bin		
	Color 1 (Red/ Red Orange)	Color 2 (Green)	Color 3 (Blue)
A	P1	R1	N1
B	P1	R1	N2
C	P1	R1	P1
D	P1	R2	N1
E	P1	R2	N2
F	P1	R2	P1
G	P1	S1	N1
H	P1	S1	N2
J	P1	S1	P1
K	P2	R1	N1
L	P2	R1	N2
M	P2	R1	P1
N	P2	R2	N1
P	P2	R2	N2
Q	P2	R2	P1
R	P2	S1	N1
S	P2	S1	N2
T	P2	S1	P1
U	Q1	R1	N1
V	Q1	R1	N2
W	Q1	R1	P1
X	Q1	R2	N1
Y	Q1	R2	N2
Z	Q1	R2	P1
1	Q1	S1	N1
2	Q1	S1	N2
3	Q1	S1	P1
4	Q2	R1	N1
5	Q2	R1	N2
6	Q2	R1	P1
7	Q2	R2	N1
8	Q2	R2	N2
9	Q2	R2	P1

Misc ID 7-05

X_6 Number of Half bins from X_5		
For HSMF-A2xx-xxxxx		
	Color 1	Color 2
0	0	0
A	0	5
B	0	4
C	0	3
D	0	2
E	5	0
F	5	5
G	5	4
H	5	3
J	5	2
K	4	0
L	4	5
M	4	4
N	4	3
P	4	2
Q	3	0
R	3	5
S	3	4
T	3	3
U	3	2
V	2	0
W	2	5
X	2	4
Y	2	3
Z	2	2

Note: 0 represents no maximum bin limit.

For HSMF-A3xx-xxxxx			
	Color 1 (Red/ Red Orange)	Color 2 (Green)	Color 3 (Blue)
0	0	0	0
A	5	5	5
B	5	5	4
C	5	5	3
D	5	4	5
E	5	4	4
F	5	4	3
G	5	3	5
H	5	3	4
J	5	3	3
K	4	5	5
L	4	5	4
M	4	5	3
N	4	4	5
P	4	4	4
Q	4	4	3
R	4	3	5
S	4	3	4
T	4	3	3
U	3	5	5
V	3	5	4
W	3	5	3
X	3	4	5
Y	3	4	4
Z	3	4	3
1	3	3	5
2	3	3	4
3	3	3	3

Note: 0 represents no maximum bin limit.

Intensity Bin Limits		
Bin ID	Min.(mcd)	Max.(mcd)
J1	4.50	5.60
J2	5.60	7.20
K1	7.20	9.00
K2	9.00	11.20
L1	11.20	14.00
L2	14.00	18.00
M1	18.00	22.40
M2	22.40	28.50
N1	28.50	35.50
N2	35.50	45.00
P1	45.00	56.00
P2	56.00	71.50
Q1	71.50	90.00
Q2	90.00	112.50
R1	112.50	140.00
R2	140.00	180.00
S1	180.00	224.00
S2	224.00	285.00
T1	285.00	355.00
T2	355.00	450.00
U1	450.00	560.00
U2	560.00	715.00
V1	715.00	900.00
V2	900.00	1125.00

Tolerance of each bin limit = ±12%.

Misc ID 7-05

Color Bin Select (X_7)
Individual reel will contain parts from 1 full bin only.

X_7	Color Bin Combinations	
For HSMF-A202-xxxxx HSMF-A203-xxxxx HSMF-A212-xxxxx HSMF-A222-xxxxx HSMF-A227-xxxxx		
	Color 1 (Red)	**Color 2 (Emerald Green/ Yellow/ Blue)**
0	0	0
A	0	ABC
B	0	ABCD
C	0	ABCDE
D	0	BCD
E	0	BCDE
F	0	BCDEF
G	0	CDE
H	0	DEF
J	0	CDEF
K	0	AB
L	0	BC
M	0	CD
N	0	DE
P	0	EF

Note: 0 represents full distribution.

For HSMF-A201-xxxxx HSMF-A211-xxxxx

	Color 1 (Red)	Color 2 (Yellow Green)
0	0	0
A	0	EFG
B	0	FGH
C	0	EF
D	0	FG
E	0	GH

Note: 0 represents full distribution.

For HSMF-A205-xxxxx HSMF-A228-xxxxx

	Color 1 (Yellow/ Amber/ Orange)	Color 2 (Emerald Green/ Blue)
0	0	0
A	ABC	ABC
B	BCD	ABC
C	CDE	ABC
D	ABC	BCD
E	BCD	BCD
F	CDE	BCD
G	ABC	CDE
H	BCD	CDE
J	CDE	CDE
K	DEF	ABC
L	DEF	BCD
M	DEF	CDE
N	AB	AB
P	BC	AB
Q	CD	AB
R	DE	AB
S	AB	BC
T	BC	BC
U	CD	BC
V	DE	BC
W	AB	CD
X	BC	CD
Y	CD	CD
Z	DE	CD
1	AB	DE
2	BC	DE
3	CD	DE
4	DE	DE
5	EF	AB
6	EF	BC
7	EF	CD

Note: 0 represents full distribution.

For HSMF-A204-xxxxx HSMF-A206-xxxxx

	Color 1 (Yellow/ Amber/ Orange)	Color 2 (Yellow Green)
0	0	0
A	ABC	EFG
B	BCD	EFG
C	CDE	EFG
D	DEF	EFG
E	ABC	FGH
F	BCD	FGH
G	CDE	FGH
H	DEF	FGH
J	AB	EF
K	BC	EF
L	CD	EF
M	DE	EF
N	EF	EF
P	AB	FG
Q	BC	FG
R	CD	FG
S	DE	FG
T	EF	FG
U	AB	GH
V	BC	GH
W	CD	GH
X	DE	GH
Y	EF	GH

Note: 0 represents full distribution.

Misc ID 7-05

For HSMF-A3xx-xxxxx	Color 1	Color 2	Color 3
0	0	0	0
A	0	0	ABC
B	0	0	BCD
C	0	0	AB
D	0	0	BC
E	0	0	CD
F	0	ABC	0
G	0	ABC	ABC
H	0	ABC	BCD
J	0	ABC	AB
K	0	ABC	BC
L	0	ABC	CD
M	0	BCD	0
N	0	BCD	ABC
P	0	BCD	BCD
Q	0	BCD	AB
R	0	BCD	BC
S	0	BCD	CD
T	0	AB	ABC
U	0	AB	BCD
V	0	AB	AB
W	0	AB	BC
X	0	AB	CD
Y	0	BC	ABC
Z	0	BC	BCD
1	0	BC	AB
2	0	BC	BC
3	0	BC	CD
4	0	CD	ABC
5	0	CD	BCD
6	0	CD	AB
7	0	CD	BC
8	0	CD	CD

Note: 0 represents full distribution.

Color Bin Limits

Blue	Min.(nm)	Max.(nm)
A	460.0	465.0
B	465.0	470.0
C	470.0	475.0
D	475.0	480.0

Green	Min.(nm)	Max.(nm)
A	515.0	520.0
B	520.0	525.0
C	525.0	530.0
D	530.0	535.0

Emerald Green	Min.(nm)	Max.(nm)
A	552.5	555.5
B	555.5	558.5
C	558.5	561.5
D	561.5	564.5

Yellow Green	Min.(nm)	Max.(nm)
E	564.5	567.5
F	567.5	570.5
G	570.5	573.5
H	573.5	576.5

Amber/ Yellow	Min.(nm)	Max.(nm)
A	582.0	584.5
B	584.5	587.0
C	587.0	589.5
D	589.5	592.0
E	592.0	594.5
F	594.5	597.0

Orange	Min.(nm)	Max.(nm)
A	597.0	600.0
B	600.0	603.0
C	603.0	606.0
D	606.0	609.0
E	609.0	612.0

Red Orange	Min.(nm)	Max.(nm)
A	611.0	616.0
B	616.0	620.0

Red	Min.(nm)	Max.(nm)
Full Distribution		

Tolerance of each bin limit = ±1 nm.

Packaging Option (X_8X_9)

X_8X_9	
J1	20 mA test current, Top Mount, 7 inch Reel

Misc ID 7-05

Misc ID 7-06

Digi International

4-23-2008

To: James Kleinke
Underwriters Laboratories, Inc.

Fax: (651) 765-1982

Subject: Letter of Assurance – National Differences

Dear James Kleinke:

This document confirms that **Digi International** was advised about the following items:

Lithium Batteries – Equipment for use in Switzerland must comply with Annex 4.10 of the latest edition of Swiss Ordinance SR 814.013 – relative to the disposal, transport of equipment containing lithium batteries, or any other applicable requirements in the said Ordinance relative to lithium batteries.

Markings and Safety Instructions – Safety instructions and markings in the language suitable for countries listed in the attached report will be provided at the time the CB Report is submitted to any Recognized NCBs to obtain Certification on the National level.

Power Supply Cords and Plugs – All Power Cord and plug assemblies will be certified and suitable for use in the particular countries when provided with the product. The recognized NCB may require certification.

EMC Test Report –Where specified in the National Difference, an EMC Test Report or Declaration of Conformity will accompany this product when sent to the Recognized NCB who requires EMC testing.

Sincerely,

Nathan Carlson

Phone: 952-912-3474
Fax:

Misc ID 7-07

Test Report issued under the responsibility of:

Working for a safer world

TEST REPORT
IEC 60 950-22
Information technology equipment
Safety – Part 22: Equipment to be installed outdoors

Report Reference No. ..... :	E165880-A46-CB-1
Date of issue ..... :	
Total number of pages	21
CB Testing Laboratory ..... :	Underwriters Laboratories, Inc.
Address ..... :	333 Pfingsten Rd, Northbrook, IL 60062
Applicant's name ..... :	DIGI International Inc.
Address ..... :	11001 Bren Rd E, Minnetonka, MN 55343
Test specification:	
Standard ..... :	IEC 60950-22 : 2005 (1st Edition)
Test procedure ..... :	CB / CCA
Non-standard test method ..... :	N/A
Test Report Form No. ..... :	IEC60950_22A
Test Report Form(s) Originator ..... :	The Standards Institution of Israel Ltd.
Master TRF ..... :	Dated 2007-03

If this Test Report Form is used by non-IECEE members, the IECEE/IEC logo and the reference to the CB Scheme procedure shall be removed.

This report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

Test item description..... :	Ethernet to Serial Converter (ConnectPort X4 NEMA)
Trade Mark ..... :	Digi
Manufacturer ..... :	Digi International
Model/Type reference ..... :	**5001544-XX**
Ratings ..... :	**100-240Vac, 47-63Hz, 25W max**

Misc ID 7-07

Testing procedure and testing location:	
☒ **CB Testing Laboratory**:	Underwriters Laboratories Inc.
Testing location/ address ..... :	333 Pfingsten Rd, Northbrook, IL 60062
☐ **Associated CB Test Laboratory:**	
Testing location/ address ..... :	
Tested by (name + signature)..... :	
Approved by (+ signature) ..... :	
☐ Testing procedure: TMP	
Tested by (name + signature)..... :	
Approved by (+ signature) ..... :	
Testing location/ address ..... :	
☐ Testing procedure: WMT	
Tested by (name + signature)..... :	
Witnessed by (+ signature) ..... :	
Approved by (+ signature) ..... :	
Testing location/ address ..... :	
☐ Testing procedure: SMT	
Tested by (name + signature)..... :	
Approved by (+ signature) ..... :	
Supervised by (+ signature)..... :	
Testing location/ address ..... :	
☐ Testing procedure: RMT	
Tested by (name + signature)..... :	
Approved by (+ signature) ..... :	
Supervised by (+ signature)..... :	
Testing location/ address ..... :	

Misc ID 7-07

Summary of testing:	
Tests performed (name of test and test clause): 1. UL/IEC 60950-1PART 22. 9.1. ANNEX B – WATER SPRAY TEST 2. Dust Test for Enclosure Designation IP6X, Clause 13.4 of IEC 60529, Edition 2.1 + Corr. 1:2003 + Corr. 2:2007 3. Water Spray Test for Enclosure Designation IPX6, Clause 14.2.6 OF IEC 60529, Edition 2.1 + Corr. 1:2003 + Corr. 2:2007 **4. Impact Test per UL60950-1 and IEC60950-1**	**Testing location:** Underwriters Laboratories Inc. 333 Pfingsten Rd, Northbrook, IL 60062
Summary of compliance with National Differences:	
Copy of marking plate: **See IEC60950-1 report**	

TRF No. IEC60950-22A

Misc ID 7-07

Test item particulars:	
Temperature range:	-40°C– 7060°C
Overvoltage category:	☐ OVC I ☒ OVC II ☐ OVC III ☐ OVC IV
IP protection class:	IP66
Possible test case verdicts:	
- test case does not apply to the test object:	N/A
- test object does meet the requirement:	P (Pass)
- test object does not meet the requirement:	F (Fail)
Testing:	
Date of receipt of test item:	2008-06-03
Date (s) of performance of tests:	2008-06-25, 2008-06-27, 2008-06-30

General remarks:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing testing laboratory.
"(see Enclosure #)" refers to additional information appended to the report.
"(see appended table)" refers to a table appended to the report.

Throughout this report a comma (point) is used as the decimal separator.

This Test Report Form is intended for the investigation of safety of equipment to be installed outdoors in accordance with IEC 60950-22. It can only be used together with the IEC 60950-1 requirements.

General product information:

ConnectPort X4 NEMA is a Ethernet to Serial converter module consisting of an Ethernet switch manufactured by Sixnet, Model SL-589 ES-123 SC ST; wireless printed Circuit Board and power supply manufactured by Bobbintron Electrical, Model AD0243-24.

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict
4	CONDITIONS FOR OUTDOOR EQUIPMENT		P
4.1	Ambient air temperature		P
	Suitability for use at any temperature in the range specified by the manufacturer. If not specified by the manufacturer, the range is taken as -33°C to +40°C		P
4.2	AC mains supply		P
	Suitability for the highest Overvoltage Category expected in the installation location	OVC II	P
	Components used to reduce the Overvoltage Category comply with IEC 61643-series		N/A
	Reference to installation instructions .....:		P
4.3	Rise of earth potential		P
	Special earthing conditions		N/A
	Reference to installation instructions .....:		P
5	MARKING AND INSTRUCTIONS		P
	Special installation features for protection from conditions in the OUTDOOR LOCATION (see 1.7.2 of IEC 60950-1)		P
	OUTDOOR ENCLOSURE classification according to IEC 60529 (IP Code)	Unit can be marked IP66 (optional)	P
6	PROTECTION FROM ELECTRICAL SHOCK IN AN OUTDOOR LOCATION		N/A
6.1	Voltage limits of user-accessible parts in OUTDOOR LOCATIONS (2.2.2 and 2.2.3 of IEC 60950-1 with voltage limits of IEC60950-22)		N/A
	Voltages under normal conditions (V).....:	See Clause 2.2.2 and 2.2.3 of IEC60950-1	N/A
	Voltages under fault conditions (V).....:	See Clause 2.2.2 and 2.2.3 of IEC60950-1	N/A
6.2	Limited current circuits in outdoor locations		N/A
	The requirements of 2.4 of IEC60950-1 apply without change	(see separate test report IEC 60950-1)	N/A

TRF No. IEC60950-22A

Misc ID 7-07

Page 6 of 24~~21~~ Report No.

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict
7	WIRING TERMINALS FOR CONNECTION OF EXTERNAL CONDUCTORS		P
	The mains supply terminations powered via the normal building installation wiring are as specified in 3.3 of IEC 60950-1		P
	The mains supply terminations powered directly from the mains distribution system are as specified in IEC 60364		N/A
8	CONSTRUCTION REQUIREMENTS FOR OURDOOR ENCLOSURES		P
8.1	General		P
	Protection against corrosion by use of suitable materials or by application of a protective coating	Polycarbonate material used in the enclosure construction	P
	Parts serving as a functional part of an OUTDOOR ENCLOSURE (e.g., dials, connectors, etc.) comply with the same environmental protection requirements as for the OUTDOOR ENCLOSURE	See Table 1.5.1 of the IEC60950-1 Report	P
	Use of OUTDOOR ENCLOSURE to carry current during normal operation	Outdoor enclosure is not designed to carry any currents during normal operation.	P
	Connection of a conductive part of an OUTDOOR ENCLOSURE to protective earth for carrying fault currents (see 2.6 of IEC 60950-1 and 8.3 of this standard)	Enclosure is constructed of non-conductive polycarbonate material, see Table 1.5.1 of IEC60950-1 report for more details.	N/A
8.2	Resistance to ultra-violet radiation		P
	Resistance of non-metallic parts of an OUTDOOR ENCLOSURE to degradation by ultra-violet (UV) radiation	See Table 1.5.1 of IEC60950-1 report for more details on the material used in the construction of the enclosure.	P
	Parts providing mechanical support:	See Table 1.5.1 of IEC60950-1 report for more details on the material used in the construction of the enclosure	P
	Tensile strength test (ISO 527)	(see appended table 8.2a)	N/A
	Flexural strength test (ISO 178)	(see appended table 8.2b)	N/A
	Parts providing impact resistance:		N/A

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict
	Charpy impact test (ISO 179)	(see appended tables 8.2c and 8.2.d)	N/A
	Izod impact test (ISO 180)	(see appended tables 8.2e and 8.2.f)	N/A
	Tensile impact test (ISO 8256)	(see appended tables 8.2g and 8.2.h)	N/A
	All parts:		N/A
	Flammability classification (1.2.12 and annex A of IEC 60950-1)	(see separate test report IEC 60950-1)	P
8.3	Resistance to corrosion		N/A
8.3.1	General		N/A
	Resistance of metallic parts of an OUTDOOR ENCLOSURE to the effects of water-borne contaminants		N/A
	Alternate method for 8.3.2-8.3.4 (IEC 61587-1)		N/A
8.3.2	Test apparatus		N/A
	Salt-spray test (IEC 60068-2-11)		N/A
	Test in a water-saturated sulphur dioxide atmosphere (water-saturated sulphur dioxide atmosphere as described in Annex A; chamber as described in ISO 3231)		N/A
8.3.3	Test procedure		N/A
8.3.4	Compliance criteria		N/A
8.4	Bottoms of FIRE ENCLOSURES		P
	Comply with 4.6.2 of IEC 60950-1		P
	Bottom of FIRE ENCLOSURE of OUTDOOR EQUIPMENT mounted directly and permanently on a non-combustible surface (e.g., concrete or metal)		P
8.5	Gaskets		P
	If gaskets are used as the method for protection against the ingress of potential contaminants, requirements of 8.5.1 through 8.5.3 apply		P
8.5.1	General		P
8.5.2	Oil resistance		P

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict
8.5.3	Securing means		P
9	PROTECTION OF EQUIPMENT WITHIN AN OUTDOOR ENCLOSURE		P
9.1	Protection from moisture (see Table 2)	Unit complies with IP66 per IEC60529 requirements and it passed the Water Spray Test per IEC 60950-22 : 2005 (1st Edition).	P
9.2	Protection from plants and vermin		N/A
9.3	Protection from excessive dust	IP6X	P

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict
10	MECHANICAL STRENGTH OF ENCLOSURES		P
10.1	General		P
10.2	Impact test (4.2.5 of IEC 60950-1)		P
	Compliance criteria:		P
	- after test the level of protection remains in accordance with 9.1of this standard		P
	- after test the requirements of 4.2.1 of IEC 60950-1 are met		P
11	OUTDOOR EQUIPMENT CONTAINING VENTED BATTERIES		N/A
	Adequate ventilation in the compartment housing a vented battery, where gassing is possible during normal usage or over-charging		N/A
	Protection against the risk of ignition of local concentrations of hydrogen and oxygen in a compartment containing both a battery and electrical components		N/A
	Hydrogen gas concentration measurement test		N/A
	Measured hydrogen gas concentration (% by volume) .....:		—
	Max. allowed gas concentration for the mixture location in proximity to an ignition source (% by volume) .....:	≤ 1% by volume	—
	Max. allowed gas concentration for the mixture location not in proximity to an ignition source (% by volume) .....:	≤ 2% by volume	—
	Overcharging of rechargeable battery (see 4.3.8 of IEC 60950-1)	(see separate test report IEC 60950-1)	N/A
A	ANNEX A, WATER-SATURATED SULPHUR DIOXIDE ATMOSPHERE (see 8.3.2 and 8.3.3)		N/A
B	ANNEX B, WATER SPRAY TEST (see 9.1)		P
C	ANNEX C, ULTRAVIOLET LIGHT CONDITIONING TEST (see 8.2)		N/A

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict
C.1	Test apparatus.....:		N/A
C.2	Mounting of test samples.....:		N/A
C.3	Carbon-arc light-exposure apparatus.....:		N/A
C.4	Xenon-arc light-exposure apparatus .....:		N/A
D	ANNEX D, GASKET TESTS (see 8.5)		N/A
D.1	Gasket tests		N/A
D.2	Tensile strength and elongation tests (for gaskets that can stretch)		N/A
	Tensile strength (%) .....:		N/A
	Elongation (%) .....:		N/A
	Visible deterioration, deformation, melting, cracking or hardening of the material.....:		N/A
D.3	Compression test (for gaskets with closed cell construction)		N/A
	Initial thickness of the specimen (mm) .....:		N/A
	Thickness of the specimen after test a) (mm), compression set after test a) (%).....:		N/A
	Thickness of the specimen after test b) (mm), compression set after test b) (%).....:		N/A
	Thickness of the specimen after test c) (mm), compression set after test c) (%).....:		N/A
	Visible cracks or deterioration .....:		N/A
D.4	Oil immersion test		N/A
	Swelling (%).....:		N/A
	Shrinking (%).....:		N/A
E	ANNEX E, RATIONALE		—
E.1	General		—
E.2	Electric shock		—
E.3	Energy related hazards		—
E.4	Fire		—

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict
E.5	Mechanical hazards		—
E.6	Heat related hazards		—
E.7	Radiation		—
E.8	Chemical hazards		—
E.9	Biological hazards		—
E.10	Explosion hazards		—

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

IEC 60950-22:2005 – COMMON MODIFICATIONS		
Contents	Add the following annexes: Annex ZA (normative) Normative references to international publications with their corresponding European publications Annex ZB (normative) Special national conditions	
General	Delete all the "country" notes in the reference document according to the following list: 4.1 Note 3 4.3 Note 8.5 Note 10.2 Note D.3 Note D.4 Note	

ZA	NORMATIVE REFERENCES TO INTERNATIONAL PUBLICATIONS WITH THEIR CORRESPONDING EUROPEAN PUBLICATIONS	—

ZB	SPECIAL NATIONAL CONDITIONS		~~N/A~~FAIL
4.1	In **Finland**, **Norway** and **Sweden**, the temperature in winter may be extremely low. For OUTDOOR EQUIPMENT this will demand special design so that the equipment can withstand transport, erection and operation/service at temperatures down to -50°C	Equipment is not Evaluated to Finland, Norway and Sweden national differences. Suitability for use in those countries has not been determined.	FAIL~~N/A~~
10.2	In **Finland**, **Norway** and **Sweden** there are additional requirements for the minimum ambient temperature. See 4.1 of this annex.	Equipment is not Evaluated to Finland, Norway and Sweden national differences. Suitability for use in those countries has not been determined.	FAIL~~N/A~~
D.3	In **Finland**, **Norway** and **Sweden** there are additional requirements for the minimum ambient temperature. See 4.1 of this annex.	Equipment is not Evaluated to Finland, Norway and Sweden national differences. Suitability for use in those countries has not been determined.	FAIL~~N/A~~

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**		
8.2a)	Tensile strength test (ISO 527)		N/A
Material identification (manufacturer, type designation) ..... :			—
Shape and dimensions of test samples..... :			—
Conditioning for Set 1 of samples ..... :			—
Conditioning for Set 2 of samples (including Annex C)..... :			—
Test conditions (T °C, RH %)..... :			—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Tensile strength (MPa)	Test sample #	Tensile strength (MPa)

Arithmetic mean for Set 1 (MPa) ..... :	
Arithmetic mean for Set 2 (MPa) ..... :	
Retention (%)..... :	

Supplementary information:

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**	
8.2b)	Flexural strength test (ISO 178)	N/A
Material identification (manufacturer, type designation) ..... :		—
Shape and dimensions of test samples..... :		—
Conditioning for Set 1 of samples ..... :		—
Conditioning for Set 2 of samples (including Annex C)..... :		—
Test conditions (T °C, RH %)..... :		—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Flexural strength (MPa)	Test sample #	Flexural strength (MPa)

Arithmetic mean for Set 1 (MPa) ..... :	
Arithmetic mean for Set 2 (MPa) ..... :	
Retention (%)..... :	

Supplementary information:

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**	
8.2c)	Charpy impact test (ISO 179) - unnotched	N/A
Material identification (manufacturer, type designation) ..... :		—
Shape and dimensions of test samples..... :		—
Conditioning for Set 1 of samples ..... :		—
Conditioning for Set 2 of samples (including Annex C)..... :		—
Test method (according to Tables 2 and 3 of ISO 179) ..... :		—
Test conditions (T °C, RH %)..... :		—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Charpy impact strength (kJ/m^2)	Test sample #	Charpy impact strength (kJ/m^2)

Arithmetic mean for Set 1 (kJ/m^2)..... :	
Arithmetic mean for Set 2 (kJ/m^2)..... :	
Retention (%)..... :	
Supplementary information:	

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**	
8.2d)	Charpy impact test (ISO 179) - notched	N/A
Material identification (manufacturer, type designation) ..... :		—
Shape and dimensions of test samples..... :		—
Conditioning for Set 1 of samples ..... :		—
Conditioning for Set 2 of samples (including Annex C)..... :		—
Test method (according to Tables 2 and 3 of ISO 179) ..... :		—
Test conditions (T °C, RH %)..... :		—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Charpy impact strength (kJ/m^2)	Test sample #	Charpy impact strength (kJ/m^2)

Arithmetic mean for Set 1 (kJ/m^2)..... :	
Arithmetic mean for Set 2 (kJ/m^2)..... :	
Retention (%)..... :	
Supplementary information:	

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**		
8.2e)	Izod impact test (ISO 180) - unnotched		N/A
Material identification (manufacturer, type designation) .....:			—
Shape and dimensions of test samples.....:			—
Conditioning for Set 1 of samples .....:			—
Conditioning for Set 2 of samples (incl. Annex C).....:			—
Test method (according to Table 1 of ISO 180) .....:			—
Test conditions (T °C, RH %).....:			—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Izod impact strength (kJ/m^2)	Test sample #	Izod impact strength (kJ/m^2)

Arithmetic mean for Set 1 (kJ/m^2).....:	
Arithmetic mean for Set 2 (kJ/m^2).....:	
Retention (%).....:	

Supplementary information:

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**		
8.2f)	Izod impact test (ISO 180) - notched		N/A
Material identification (manufacturer, type designation) .....:			—
Shape and dimensions of test samples.....:			—
Conditioning for Set 1 of samples .....:			—
Conditioning for Set 2 of samples (incl. Annex C).....:			—
Test method (according to Table 1 of ISO 180) .....:			—
Test conditions (T °C, RH %).....:			—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Izod impact strength (kJ/m^2)	Test sample #	Izod impact strength (kJ/m^2)

Arithmetic mean for Set 1 (kJ/m^2).....:	
Arithmetic mean for Set 2 (kJ/m^2).....:	
Retention (%).....:	

Supplementary information:

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**		
8.2g)	Tensile impact test (ISO 8256) - unnotched		N/A
Material identification (manufacturer, type designation) .....:			—
Shape and dimensions of test samples.....:			—
Conditioning for Set 1 of samples .....:			—
Conditioning for Set 2 of samples (incl. Annex C).....:			—
Test method (A or B) .....:			—
Test conditions (T °C, RH %).....:			—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Tensile impact strength (kJ/m^2)	Test sample #	Tensile impact strength (kJ/m^2)

Arithmetic mean for Set 1 (kJ/m^2).....:	
Arithmetic mean for Set 2 (kJ/m^2).....:	
Retention (%).....:	

Supplementary information:

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

8.2	**TABLE: Resistance to ultra-violet radiation**		
8.2h)	Tensile impact test (ISO 8256) - notched		N/A
Material identification (manufacturer, type designation) .....:			—
Shape and dimensions of test samples.....:			—
Conditioning for Set 1 of samples .....:			—
Conditioning for Set 2 of samples (incl. Annex C).....:			—
Test method (A or B) .....:			—
Test conditions (T °C, RH %).....:			—

Set 1 (without Annex C conditioning)		Set 2 (after Annex C conditioning)	
Test sample #	Tensile impact strength (kJ/m^2)	Test sample #	Tensile impact strength (kJ/m^2)

Arithmetic mean for Set 1 (kJ/m^2).....:	
Arithmetic mean for Set 2 (kJ/m^2).....:	
Retention (%).....:	
Supplementary information:	

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

TRF No. IEC60950-22A

Misc ID 7-07

IEC 60950-21			
Clause	Requirement + Test	Result - Remark	Verdict

List of test equipment used (required when MTL equipment is used):
(Note: This is an example of the required attachment. Other forms with a different layout but containing similar information are also acceptable.)

Inst. ID No.	Instrument Type	Test Number +, Test Title or Conditioning	Function/Range	Last Cal. Date	Next Cal. Date

Enclosure

Licenses

Supplement Id	Description
8-02	Power Supply
8-03	European Plug VDE certificate

License ID 8-02

	Ref. Certif. No.
IEC IECEE CB SCHEME	DK-13441

IEC SYSTEM FOR MUTUAL RECOGNITION OF TEST CERTIFICATES FOR ELECTRICAL EQUIPMENT (IECEE) CB SCHEME

SYSTEME CEI D'ACCEPTATION MUTUELLE DE CERTIFICATS D'ESSAIS DES EQUIPEMENTS ELECTRIQUES (IECEE) METHODE OC

CB TEST CERTIFICATE
CERTIFICAT D'ESSAI OC

Product Produit	Switching Power Supply
Name and address of the applicant Nom et adresse du demandeur	BOBBINTRON ELECTRICAL CORP 19TH FL 38 LIEN-HSIN ST, HSI CHIH, TAIPEI HSIEN 22167, TAIWAN
Name and address of the manufacturer Nom et adresse du fabricant	BOBBINTRON ELECTRICAL CORP 19TH FL 38 LIEN-HSIN ST, HSI CHIH, TAIPEI HSIEN 22167, TAIWAN
Name and address of the factory Nom et adresse de l'usine Note: *When more than one factory, please report on page 2* Note: *Lorsque il y plus d'une usine veuillez utiliser la 2ème page*	GAIN SOUTH ELECTRONIC (SHENZHEN) LTD BLDG 15, HEDONG II INDUSTRIAL AREA, BAO'AN DISTRICT, XIXIANG, SHENZHEN GUANGDONG, CHINA
Ratings and principal characteristics Valeurs nominales et caractéristiques principales	100-240 Vac, 50 - 60 Hz, 0.7 A; Class I, IP X0
Trademark (if any) Marque de fabrique (si elle existe)	bec
Model / Type Ref Ref. De type	AD0243-24
Additional information (if necessary may also be reported on page 2) Les informations complémentaires (si nécessaire, peuvent être indiqués sur la 2ème page)	for building-in, Output: 24 Vdc / 1.0 A. Also investigated to EN 60950-1:2001+A11:2004
A sample of the product was tested and found to be in conformity with Un échantillon de ce produit a été essayé et a été considéré conforme à la	**PUBLICATION** / **EDITION** IEC 60950-1:2001 / 1st
As shown in the Test Report Ref. No. which forms part of this Certificate Comme indiqué dans le Rapport d'essais numéro de référence qui constitue partie de ce Certificat	E235661-A15-CB-1 issue date 2008-06-12 with Correction 1 issue date 2008-06-13

This CB Test Certificate is issued by the National Certification Body
Ce Certificat d'essai OC est établi par l'Organisme **National de Certification**

Underwriters Laboratories

Date: 2008-06-13

UL International Demko A/S
Lyskaer 8, P.O. Box 514, DK-2730 Herlev, Denmark
Tel: +45 44856565, Fax: +45 44856500

Signature:

Jan-Erik Storgaard
Certification manager

License ID 8-03

VDE Prüf- und Zertifizierungsinstitut

ZEICHENGENEHMIGUNG
MARKS APPROVAL

Yung-Li Co. Ltd.
Da Pu Industrial Zone
Chang Ping Town
523571 Dong Guan City
Guangdong
CHINA

ist berechtigt, für ihr Produkt /
is authorized to use for their product

Stecker mit Schutzkontakt, nicht wiederanschließbar, umspritzt
Plug, with earthing contact, non-rewirable, moulded
YP-22

die hier abgebildeten markenrechtlich geschützten Zeichen
für die ab Blatt 2 aufgeführten Typen zu benutzen /
the legally protected Marks as shown below for the types referred to on page 2 ff.

Geprüft und zertifiziert nach /
Tested and certified according to

DIN VDE 0620-1 (VDE 0620-1):2005-04

Aktenzeichen: 1609800-1560-0002 / 65698
File ref.:
Ausweis-Nr. 40003878 Blatt 1
Certificate No. *Page*
Weitere Bedingungen siehe Rückseite und Folgeblätter /
further conditions see overleaf and following pages

Offenbach, 2002-11-04
(letzte Änderung/updated 2006-01-26)

VDE Prüf- und Zertifizierungsinstitut
VDE Testing and Certification Institute
Zertifizierungsstelle / *Certification*

VDE Zertifikate sind nur gültig bei Veröffentlichung unter:
VDE certificates are valid only when published on:
http://www.vde.com/zertifikat
http://www.vde.com/certificate

VDE VERBAND DER ELEKTROTECHNIK
ELEKTRONIK INFORMATIONSTECHNIK e.V.

License ID 8-03

VDE Prüf- und Zertifizierungsinstitut Zeichengenehmigung

Ausweis-Nr. / Certificate No. 40003878 | Blatt / page 2

Name und Sitz des Genehmigungs-Inhabers / *Name and registered seat of the Certificate holder*
Yung-Li Co. Ltd., Da Pu Industrial Zone, Chang Ping Town, 523571 Dong Guan City, Guangdong, CHINA

Aktenzeichen / *File ref.*
1609800-1560-0002 / 65698 / FG33 / E

letzte Änderung / *updated* 2006-01-26

Datum / *Date* 2002-11-04

Dieses Blatt gilt nur in Verbindung mit Blatt 1 des Zeichengenehmigungsausweises Nr. 40003878.
This supplement is only valid in conjunction with page 1 of the Certificate No. 40003878.

Stecker mit Schutzkontakt, nicht wiederanschließbar, umspritzt
Plug, with earthing contact, non-rewirable, moulded
YP-22

Typ(en) / *Type(s)*:

YP-22

Bemessungsspannung *Rated voltage*	AC 250 V
Bemessungsstrom *Rated current*	16 A
Polzahl *Number of poles*	2-polig mit zwei Schutzkontaktsystemen *2-pole with two earthing contact systems*
Bauart *Kind of construction*	Normblatt: DIN 49441-R2 *standard sheet: DIN 49441-R2*
Schutzart *Degree of protection*	IP20
Technische Daten *Technical data*	siehe Anlage Nr. 400A *see Appendix No. 400A*

VDE Prüf- und Zertifizierungsinstitut
VDE Testing and Certification Institute
Fachgebiet FG33
Section FG33

i.A. i.A.

VDE Testing and Certification Institute * Institut VDE d'Essais et de Certification
Merianstrasse 28, D-63069 Offenbach
Phone +49 (0) 69 83 06-0
Telefax +49 (0) 69 83 06-555

License ID 8-03

Certificate no. 312073-01

Demko Certificate

Product:	Non-rewirable two-pole plug
Manufacturer:	Yung Li Co., Ltd. 1F, No. 10, Lane 235, Pao-Chiang Rd., Hsin-Tien, Taipei, TAIWAN
Production site:	Yung Li Co.; Ltd. China Da Pu Industrial Zone, Chang Ping Town, Dong Guan City, Guang Dong Province, P.R. CHINA
Certified by request of:	Same as manufacturer
Trademark:	YUNG LI
Model/Type ref.:	YP-22
Rated current or power:	16 A
Rated voltage:	250 V AC
Insulation Class:	-
Degree of protection:	-
Additional information:	Thermoplastic. Standard sheet VII.

Variants covered by this certificate are specified in the attached appendix.
Detailed specification of the certified product(s) is listed in the appendix.

A sample of the product has been tested and found in conformity with IEC 60884-1 Ed.2 (1994) A1 + (1995) A2 + CEE 7 with Mod. 1-3 + EMKO TSI(23B)FI 226/92-12

Date of expiry: 2013-01-15.

Furthermore, the product complies with the national deviations in Denmark.

UL International Demko A/S is a body notified to the Member States and Commission of the European Communities according to the provisions of Article 8 of the Low Voltage Directive.
The Manufacturer complies with the Production Surveillance Requirements.
Products included in this certificate are allowed to carry the registered approval marks of UL International Demko A/S, ⓓ or for cables ◁DEMKO▷. The name of UL International Demko A/S can be used in the marketing of the products as well.
This certificate is only valid for products, which are identical to the certified product, and manufactured at the above mentioned production site(s). UL International Demko A/S has to be informed in writing about any changes, in accordance with the "UL International Demko A/S Standard Terms and Conditions" for UL International Demko A/S services.

Herlev, 2003-02-25

Karina Christiansen
Certification Manager

UL International Demko A/S
Lyskaer 8, P.O. Box 514
DK-2730 Herlev, Denmark
Telephone: +45 44856565
Fax: +45 44856500

An Affiliate of Underwriters Laboratories Inc.®

License ID 8-03

Appendix to
Demko Certificate No. 312073–01

The Certificate covers the following:

01; YP-22; with H 03 VV-F 3 G 0.75 mm²

02; YP-22; with H 05 VV-F 3 G 0.75-1.5 mm²

The certificate has been issued on the basis of Nordic certification Service, certificate No. P03100059, issued by Nemko, dated 2003-01-15.

Herlev, 2003-02-25

Karina Christiansen
Certification Manager

UL International Demko A/S
Lyskaer 8, P.O. Box 514
DK-2730 Herlev, Denmark
Telephone: +45 44856565
Fax: +45 44856500

An Affiliate of
Underwriters
Laboratories Inc.®

License ID 8-03

Nemko

CERTIFICATE

No. P03100059

Order No. 200302284

Applicant	Yung Li Co., Ltd. 1F, No. 10, Lane 235 Pao-Chiang Rd., Hsin-Tien Taipei TAIWAN
Manufacturer	Yung Li Co., Ltd. 1F, No. 10, Lane 235 Pao-Chiang Rd., Hsin-Tien Taipei TAIWAN
Factory	Yung Li Co., Ltd. China Da Pu Industrial Zone, Chang Ping Town Dong Guan City, Guang Dong Province P.R. CHINA
Group 03 43000	Non-rewirable two-pole plug with dual earthing-contacts. Standard Sheet VII
Model/type	YP-22
Data	16A 250V AC
Other specification	Thermoplastic, with H03VV-F 3G0,75mm^2
The above product is certified according to the following standard(s)	Safety std.: NEK-IEC 60884-1 :94 + A1 :94 + A2 :95 + relevant parts of CEE7
Validity	This certificate documents conformity with the standards shown, and also applies as license for use of Nemko's name and certification mark. The certificate and license is valid as long as the applicable conditions are complied with, and provided that any changes to the product are notified to Nemko for acceptance prior to implementation. New standards or amendments to the standards may imply that the product design must be updated and/or that re-testing and re-certification is necessary.
Variants	This Certificate also covers variant with Position No. 001 See next page

Date of issue 15 January 2003

signature

Ragnar Køltzow

Certification Department

Nemko AS P.O. Box 73, Blindern N-0314 Oslo, Norway	Office address Gaustadalléen 30 Oslo	Telephone +47 22 96 03 30 Enterprise number:	Fax +47 22 96 05 50 NO 974404532

License ID 8-03

Nemko

CERTIFICATE

No. P03100059

Order No. 200302284

Group 03 43000	Non-rewirable two-pole plug with dual earthing-contacts. Standard Sheet VII
Position No	001
Model/type	YP-22
Data	16A 250V AC
Other specification	Thermoplastic, with H05VV-F 3G0,75-1,5mm^2

Date of issue 15 January 2003

signature

Ragnar Køltzow

Certification Department

Nemko AS	Office address	Telephone	Fax
P.O. Box 73, Blindern	Gaustadalléen 30	+47 22 96 03 30	+47 22 96 05 50
N-0314 Oslo, Norway	Oslo	Enterprise number:	NO 974404532

License ID 8-03

Certificate

Product Safety

- with the right to S marking

Reference No / Referensnr. 304216

Plug, non rewirable

Type designation / Typbeteckning	YP-22
Manufacturer / Certifikatsinnehavare	**YUNG LI CO., LTD.** **1F, No. 10, Lane 235** **Pao-Chiao Road, Hsin-Tien, Taipei** **Taipei Hsien** **TAIWAN**
The product complies with the standard(s) / Produkt uppfyller standard	IEC 60884-1:1994 and A1+A2 SS 428 08 34:1998
Date of expiry / Giltigt längst t o m	31 December 2013

Terms in SEMKO's Agreement on certification. Additional information in Appendix.

Certification Body / Certifieringsorgan SEMKO AB, Product Certification

Place / Ort Kista - Stockholm

Signed / Underskrift Pär Zetterberg

Date / Datum 8 April 2003

ITS Intertek Testing Services
ETL SEMKO

License ID 8-03

SEMKO

Appendix

Reference No / Referensnr. 304216

Technical data /Tekniska data	
Type designation / Typbeteckning	YP-22
Rated Voltage (V) / Märkspänning	250
Rated Current (A) / Märkström	16
IP-Class / IP-Klass	20
Type of Cord / Kabeltyp	H03VV-F
Number of Conductors / Ledarantal	3G
Conductor Area / Ledararea	0,75mm²
Standard sheet / Normblad	CEE7/VII

Manufacturing site(s) / Tillverkningsställe(n)

YUNG LI CO. LTD. CHINA
Da Pu Industrial Zone
Chang Ping Town
Dongguan City, Guang Dong
511736
CHINA

This certificate is based on a certificate with ref. No. 200302284 dated 15 January 2003, issued by NEMKO according to the Nordic Certification Service Agreement.

Kista/Stockholm
8 April 2003

Pär Zetterberg

Page / Sid 1 (1)

ITS Intertek Testing Services
ETL SEMKO

License ID 8-03

KEMA

KEMA KEUR

CERTIFICATE

KEMA No.: **2026550.01**

Issued to:
Applicant:
Yung Li Co. Ltd.
1F,No.10,Lane 235
HSIN-TIEN, TAIPEI COUNTY, Taiwan

Manufacturer/Licensee:
Yung Li Co. Ltd.
1F,No.10,Lane 235
HSIN-TIEN, TAIPEI COUNTY, Taiwan

Product : plug, (2-pole)

Trade names : YUNG LI, YUNG-LI
Type/model : YP-22

The product and any acceptable variation thereto is specified in the Annex to this certificate and the documents therein referred to.

KEMA hereby declares that the above-mentioned product has been certified on the basis of:
- a type test according to the standard IEC 60884-1:1994+A1:94+A2:95
- an inspection of the production location according to CENELEC Operational Document CIG 021
- a certification agreement with the number 956361

KEMA hereby grants the right to use the KEMA-KEUR certification mark

KEMA KEUR

The KEMA-KEUR certification mark may be applied to the product as specified in this certificate for the duration of the KEMA-KEUR certification agreement and under the conditions of the KEMA-KEUR certification agreement.

This certificate is issued on: January 20, 2003

H.R.M. Barends
Certification Manager

KEMA Quality B.V.
Utrechtseweg 310, 6812 AR Arnhem, The Netherlands
P.O. Box 5185, 6802 ED Arnhem, The Netherlands
Telephone +31 26 3 56 20 00, Telefax +31 26 3 52 58 00

ACCREDITED BY
THE DUTCH COUNCIL
FOR ACCREDITATION

License ID 8-03

KEMA

ANNEX TO KEMA-KEUR CERTIFICATE 2026550.01 page 1 of 1

SPECIFICATION OF THE CERTIFIED PRODUCT

Product data

Product	:	plug, (2-pole)
trade names	:	YUNG LI,YUNG-LI
type	:	YP-22
rated current	:	16 A
rated voltage	:	250 V~
earthing	:	with dual earthing contacts
design	:	non-rewirable
standard sheet	:	VII
applied flexible cord	:	H03VV-F 3G0,75 mm² H05VV-F 3G0,75, 3G1,0 and 3G1, 5 mm²
certification mark	:	KEMA-KEUR
cord termination	:	crimped connection
description	:	angled type, body of thermoplastic material as part of an incomplete cord set for class I appliances
markings	:	are shown on the body

TESTS

Test requirements
NEN 1020, 4th.ed.:1987 + A1:1998 (based on IEC 60884-1)

Test results
The test results are laid down in CB No. DE 1 - 19394 and TRF No. 1609800-1560-0002/15244.

Remarks
This KEMA-KEUR Certificate replaces the Certificate No. 95.8361.01 and is also based on CB Certificate No. DE1-19394

Conclusion
The examination proved that all test requirements were met.

Tested by : VDE

Checked by : H.R.M. Barends

Factory-Location
Yung-Li Co., Ltd.,
Da Pu, Industrial Zone, DONG GUAN CITY, CHINA

KEMA Quality B.V.
Utrechtseweg 310, 6812 AR Arnhem, The Netherlands
P.O. Box 5185, 6802 ED Arnhem, The Netherlands
Telephone +31 26 3 56 20 00, Telefax +31 26 3 52 58 00

License ID 8-03

CEBEC

LICENCE

No. 12989 replaces No.8582

Issued to:
Applicant:
Yung Li Co. Ltd.
1F, No.10, Lane 235,
Pao Chiang Road
HSIN-TIEN, TAIPEI
Taiwan

Licensee:
Yung Li Co. Ltd.
1F, No.10, Lane 235,
Pao Chiang Road
HSIN-TIEN, TAIPEI
Taiwan

Product	:	plugs (2-pole) for household purposes
Trade name(s)	:	YUNG-LI
Type(s)/model(s)	:	YP-22

The product and any acceptable variation thereto is specified in the annex to this licence and the documents therein referred to.

CEBEC hereby declares that the above-mentioned product has been certified on the basis of:
- a type test according to the standard specified in annex
- an inspection of the production location according to CCA Group Operational Document CIG 021
- a certification agreement with the number 1031

CEBEC hereby grants the right to use the CEBEC certification mark

CEBEC

The CEBEC certification mark may be applied to the product as specified in this licence for the duration of the CEBEC certification agreement and under the conditions of the CEBEC certification agreement.

This licence is issued on: 13/01/2003

ir. R. Maquestiau,
Managing Director

Only integral publication of this certificate, including the annex, is allowed

CEBEC scrl/cvba
Avenue F. Van Kalkenlaan, 9A/b 1
B-1070 Brussel/Brussel
t: +32 [0]2 556 00 20
f: +32 [0]2 556 00 36

Accredited by BELCERT 041 PR

License ID 8-03

CEBEC

ANNEX TO CEBEC LICENCE No. 12989

SPECIFICATION OF THE CERTIFIED PRODUCT

Product data

Product	:	plugs (2-pole) for household purposes
Trade name(s)	:	YUNG-LI
Type(s)/Model(s)	:	YP-22
rated current (In)	:	16 A
rated voltage (Un)	:	250 Vac
earthing	:	with dual earthing system
design	:	non-rewirable
class	:	for class I appliances
standard sheet	:	VII
applied flexible cord(s)	:	H03 VV-F 3G0.75 mm² H05 VV-F 3G0.75-1-1.5 mm²
certification mark	:	complies with the requirements
cord(s) termination	:	crimped connection
description	:	body of thermoplastic material as part of an incomplete cord set for class I appliances
markings	:	are shown on the body

TESTS

Test requirements

NBN C 61-112-1:1990 + A1:1993 + A2:1995 + A3:1999 + A4:2001

Test results

The test results are laid down in certification file ref.575528/01

Remarks

This certificate is based on certificate ref. CB VDE 1-19394 and test report(s) ref. 1609800-1560-0002/15244

CEBEC
Avenue F. Van Kalkenlaan, 9A
Bruxelles B-1070 Brussel

Telephone +32 2 5560020, Telefax +32 2 5560036

575528/01

License ID 8-03

SGS Fimko Ltd
Särkiniementie 3, P.O. Box 30
FIN-00211 Helsinki, Finland
Phone +358 9 696 361
Fax +358 9 692 5474
e-mail: sgs_fimko@sgs.com

Our Ref. 227798-01

CERTIFICATE FI 19608

Product	Plug, non-rewirable
Type	YP-22, with cord H03VV-F 3G0,75 YP-22, with cord H05VV-F 3G0,75-1-1,5
Trade mark	YUNG LI
Certificate Holder/ Manufacturer	Yung Li Co., Ltd. 1F, No. 10, Lane 235 Pao-Chiag Rd., Hsin-Tien 231 TAIPEI TAIWAN
Technical information	16 A, 250 V~, IP 20
Other information	Standard sheet CEE 7 / VII
The product is certified according to the following standard(s)	IEC 60884-1:1994 + A1:1994 + A2:1995 SFS 5610:1996 + A1:1998
Validity	This certificate is valid until 31 December 2013 unless the standard in question has been amended or superseded with significant changes in requirements, in which case, SGS Fimko has the right to shorten the validity of the certificate based on the legislation of the European Union. This certificate includes the right to use the FI mark under the condition that changes (if any) will be checked at SGS Fimko before the product is brought onto market and that the conditions for FI certification are met.
Date of issue	05 May 2003
	SGS Fimko Ltd
Signature	Osmo Väyrynen Certification Manager

This certificate has 1 appendix

License ID 8-03

IMQ S.p.A.
I-20138 Milano - via Quintiliano, 43
tel. 0250731(r.a.) - fax 0250991500
e-mail: info@imq.it - www.imq.it

Rea Milano 1595884
Registro Imprese MI 12898410159
C.F./P.I.12898410159
Capitale Sociale € 3.925.400

CA02.01593
SN.D000DL

PID:
02113100
CID:
C.1996.5269

Certificato di approvazione

Approval certificate

IMQ, ente di certificazione accreditato, autorizza la ditta

IMQ, accredited certification body, grants to

YUNG LI CO., LTD.
1F, N.10, LANE 235, PAO CHIANG RD., HSIN-TIEN
231
TAIPEI
TW - Taiwan

all'uso del marchio

the licence to use the mark

IMQ

Il presente certificato è soggetto alle condizioni previste nel "Regolamento IMQ - Certificazione prodotto" ed è relativo ai prodotti descritti nell'Allegato al presente certificato.

per i seguenti prodotti

Spine indissolubilmente collegate al cavo
(Rif. di tipo YP-22)

for the following products

Non-rewirable plugs
(Type ref. YP-22)

This certificate is subjected to the conditions foreseen by "IMQ Rules - Product Certification" and is relevant to the products listed in the annex to this certificate.

Emesso il / Issued on:
2003-04-17
Data di aggiornamento / Updated on

Sostituisce / Replaces

IMQ S.p.A.

License ID 8-03

IMQ

CA02.01593
SN.D000DL

Marca | Trade mark **YUNG-LI**
Rif. di tipo | Type ref. **YP-22**
Tipo di cavo | Type of cable **H05VV-F**
Sezione nominale | Section areas **3G1,50mm²**

Diritti di concessione | Annual Fees

SN.D000DL BTO.021109.0419 *Diritti modelli IMQ - 0211 - Prese, spine e connettori di uso domestico | IMQ models - 0211 - Plugs and appliance couplers for domestic purposes* 1

IMQ S.p.A.

2/2

IMQ

CA02.01593
SN.D000DL

Allegato - Certificato di approvazione
Annex - Approval certificate

Emesso il | Issued on 2003-04-17
Data di aggiornamento | Updated on
Sostituisce | Replaces

Prodotto | Product

Spine indissolubilmente collegate al cavo
Non-rewirable plugs

Concessionario | Licence Holder

YUNG LI CO., LTD.
1F, N.10, LANE 235, PAO CHIANG RD., HSIN-TIEN 231
TAIPEI
TW - Taiwan

Marchio | Mark

Costruito a | Manufactured at

DONG GUAN CITY, GUANG DONG PROV. China

Copia del presente certificato deve essere conservata presso i luoghi di produzione sopra elencati.

Copy of this certificate must be available at the manufacturing places listed above

Norme **Standards**

CEI 23-50 - I Ed. 1998 + V1:2002 *CEI 23-50 - I Ed. 1998 + V1:2002*

Rapporti | Test Reports

02AD00008

Caratteristiche tecniche | Technical characteristics

Designazione | Type designation **2P+T+T S31 / 2P+E+E S31**
Tensione nominale | Rated voltage **250V**
Corrente nominale | Rated current **16A**
Grado di protezione | Degree of protection (IP) **IPX0**
Tipo di morsetti | Type of terminals **MA = morsetti aggraffati / MA = crimped connection**
Materiale della custodia | Material of the cover **termoplastico / thermoplastic**
Uscita cavo | Cable exit **a squadra / angled**

Articoli (con dettagli) | Articles (with details)

Marca | Trade mark **YUNG-LI**
Rif. di tipo | Type ref. **YP-22**
Tipo di cavo | Type of cable **H03VV-F**
Sezione nominale | Section areas **3G0,75mm²**

Marca | Trade mark **YUNG-LI**
Rif. di tipo | Type ref. **YP-22**
Tipo di cavo | Type of cable **H05VV-F**
Sezione nominale | Section areas **3G0,75mm²**

Marca | Trade mark **YUNG-LI**
Rif. di tipo | Type ref. **YP-22**
Tipo di cavo | Type of cable **H05VV-F**
Sezione nominale | Section areas **3G1mm²**

1/2

License ID 8-03

AUSTRIAN ELECTROTECHNICAL ASSOCIATION
1010 Wien, Eschenbachgasse 9

Testing & Certification
Kahlenberger Str. 2A
1190 Wien, Austria
Telefon: +43 1 370 58 06
Telefax: +43 1 817 495 542 27

ÖVE-CERTIFICATE

including the entitlement to use the Austrian Safety Mark

Certificate No.: **12396-011-02**

Valid from: 2007 02 17
until: 2009 02 17

The Austrian Electrotechnical Association (ÖVE) hereby grants the right to the company mentioned below to label the listed products with the Austrian Safety Mark.

Company: **YUNG LI CO. LTD.**
1F., No. 10, Lane 235, Pao-Chiang Road,
Hsin-Tien Taipei
Taiwan

Product: **Non rewireable two pole plug with dual earthing system**

Basis for this given right is the conformity of the products with the requirements of the technical standards listed in this certificate as shown in the test report
Ref.-No. **1740-1182/03**.

This certificate establishes the conformity of the tested specimen and of all products manufactured strictly identical to the submitted one.

ÖSTERREICHISCHER VERBAND FÜR ELEKTROTECHNIK
Head of Testing & Certification

Vienna, 2007 01 30 Dipl.-Ing. W. Martin

OVE - Testing & Certification

Accredited by the Austrian Ministry of Economics and Labour as Certification Body and Inspection Body for products, process and system evaluation in the whole field of electrotechnology

License ID 8-03

Österreichischer Verband für Elektrotechnik OVE

Certificate No.: 12396-011-02
Date: 2007 01 30
Page 2 of 2

Manufacturer:

Yung Li Co. Ltd.
Da Pu Industrial Zone, Gang Zi, Chang Ping Town
523571 Dong Guan City, Guang Dong Province
China

Factory location(s):

Yung Li Co. Ltd.
Da Pu Industrial Zone, Gang Zi, Chang Ping Town
523571 Dong Guan City, Guang Dong Province
China

Tested and certified according to:

ÖVE/ÖNORM IEC 60884-1:2000-03-01

Product: Non rewireable two pole plug with dual earthing system

Type designation: *Rating:*	***Trademark:***
YP-22 Rated voltage: AC 250 V Rated current: 16 A H03VV-F 3 G 0,75	YUNG LI
YP-22 Rated voltage: AC 250 V Rated current: 16 A H05VV-F 3 G 0,75	YUNG LI
YP-22 Rated voltage: AC 250 V Rated current: 16 A H05VV-F 3 G 1	YUNG LI
YP-22 Rated voltage: AC 250 V Rated current: 16 A H05VV-F 3 G 1,5	YUNG LI

Österreichischer Verband für Elektrotechnik
Sektion
Prüfwesen & Zertifizierung ÖVE

OVE - Testing & Certification

Accredited by the Austrian Ministry of Economics and Labour as Certification Body and Inspection Body for products, process and system evaluation in the whole field of electrotechnology

License ID 8-03

Accréditation
N° 5-0014

LICENCE

LCIE N° 555296

Délivrée à: *Delivered to:*	**YUNG LI Co., Ltd** 1F, No 10, Lane 235 , Pao-Chiang Road , Hsin-Tien - TAIPEI - TAIWAN
Site de fabrication : *Factory :*	**YUNG LI Co., Ltd.** **(1532AP)** Da Pu Industrial Zone, Gang Zi, Chang Ping Town - Dong Guan City - GUANG DONG PROVINCE 523571 - CHINE
Produit: *Product:*	FICHE DE PRISE DE COURANT *PLUG*
Marque commerciale (s'il y a lieu): *Trade mark (if any):*	**YUNG-LI**
Modèle, type, référence: *Model, type, reference:*	YP-22
Caractéristiques nominales et principales: *Rating and principal characteristics:*	16A, 250V~, 2P+T/*2P+E* , non démontable/*non-rewirable*, toutes couleurs/*all colors*, entrée latérale de câble/*lateral entry of cable* H03VV-F 3G0,75 ou/*or* H05VV-F 3G0,75 - 3G1,0 - 3G1,5mm²
Informations complémentaires: *Additional informations:*	câbles fabriqués par / *cables manufactured by* : YUNG LI CO. LTD certifiés/*certified* NF-USE
Le produit est conforme à: *The product is in conformity with:*	NF C 61-314:2003
Documents pris en compte: *Relevant documents:*	Rapport d'essai/test report LCIE n° YLC06DE142ACSP
Annule et remplace (s'il y a lieu): *Cancels and replaces (if necessary):*	/

Cette licence autorise l'usage de la marque NF pour le produit dans les conditions du règlement de la marque NF, pour autant que les contrôles réguliers de la fabrication et les vérifications par tierce partie soient satisfaisants.

Fontenay-aux-Roses, 2007-02-08

Date limite de validité :
Limit expired date :

La validité de la présente licence cesse dès l'annulation de l'une des normes sur laquelle elle est fondée.
The present licence is valid until the cancellation of one of the standards on which it is based.

This licence permits the use of the Mark NF for the product in compliance with the Regulation of the NF Mark, as far as the regular checking and third party verifications of the production are satisfactory.

Par mandatement de AFAQ AFNOR Certification et pour le LCIE
By mandate from AFAQ AFNOR Certification and for LCIE

Michel BRENON
Responsable de certification
Certification manager

dtcr-nf-1.3

LCIE
Laboratoire Central
des Industries Electriques
Une société de Bureau Veritas

33, av. du Général Leclerc
BP 8
92260 Fontenay-aux-Roses cedex
France

Tél : +33 1 40 95 60 60
Fax : +33 1 40 95 86 56
contact@lcie.fr
www.lcie.fr

Société Anonyme
au capital de 15 745 984 €
RCS Nanterre B 408 363 174