ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Find the *Ribbon / Performance Technologies PT-CPC4416F* at our website: *Click HERE*

CPC441x

Ethernet Switching Platform

User's and System Integrator's Guide

Performance Technologies
205 Indigo Creek Drive
Rochester, NY 14626
585.256.0200
support@pt.com

www.pt.com

© 2009 Performance Technologies, Inc.
All Rights Reserved.

PERFORMANCE TECHNOLOGIES

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Document Revision History

CPC441x Ethernet Switching Platform User's Guide, part number: 126p0433

Revision	Date	Explanation of Changes
10	November 21, 2003	Initial release
11	April 9, 2004	CLI updates
20	July 9, 2004	Application code updates
21	July 16, 2004	Boot file upgrade procedure
22	February 16, 2005	CLI updates
30	March 18, 2005	Application code updates
40	April13, 2006	Application code updates
41	April 25, 2007	DRAFT - Errata Corrections
42	February 28, 2008	CLI Updates - VLANs, SNMP. SNMPv3 updates. Added Lua and traceroute Licence Agreements. Added Fault State note. Reformatted manual.
43	April 24, 2009	Miscellaneous updates for Release 5.5.35 and 5.6: CLI commands, Lua commands, DHCP Vendor Options, Message of the Day files. Corrected Set Maximum Delay.

Copyright Notice

© Copyright 2009 by Performance Technologies, Inc. All Rights Reserved.

The Performance Technologies logo is a registered trademark of Performance Technologies, Inc. All other product and brand names may be trademarks or registered trademarks of their respective owners.

This document is the sole property of Performance Technologies Inc.

Warning

Laser light may be emitted from fiber-optic transmission cables and components. To avoid damaging your eyes:

- Never look directly with the naked eye into the outlets of fiber-optic cables or fiber-optic transmission components.
- Never allow fiber-optic transmission paths to operate until all the connections have been made.
- Never leave unused connections on the switch or network card exposed; fit protective plugs.

The laser components in the fiber-optic interfaces are Class 1 laser components.

Certifications

The CPC441x is certified as indicated in the following sections. If a certification is not listed below, the CPC441x may still comply. Contact Performance Technologies for current product certifications and availability.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

FCC (USA) Class A Notice

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

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial 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. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Modifications made to this device that are not approved by Performance Technologies may void the authority granted to the user by the FCC to operate this equipment.

CE Notice

CE

The product(s) described in this manual conform to the ***EU 89/336/EEC Electromagnetic Compatibility Directive***, amended by ***92/31/EEC*** and ***93/68/EEC***.

The product described in this manual is:

- CPC441x

The product identified above complies with the **EU 89/336/EEC** Electromagnetic Compatibility Directive by meeting the applicable EU standards as outlined in the Declaration of Conformance. The **Declaration of Conformance** is available from Performance Technologies, Inc. or from your authorized distributor.

ETSI EN 300 386

Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) Requirements.

ISO 9002 Notice

Performance Technologies, Inc., is registered by BVQI as ISO 9002 compliant.

Safety Certifications

EN60950-1: 2001

UL60950-1

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Errors and Omissions

Although diligent efforts are made to supply accurate technical information to the user, occasionally errors and omissions occur in manuals of this type. Refer to the Performance Technologies, Inc. Web site to obtain manual revisions or current customer information:

http://www.pt.com.

Performance Technologies, Inc., reserves its right to change product specifications without notice.

Symbols and Conventions in this Manual

An overbar indicates the signal is an active low signal.

Example: $\overline{\text{ENUM}}$

The following symbols may appear in this document.



Caution:
There is risk of personal injury or equipment damage. Follow the instructions.



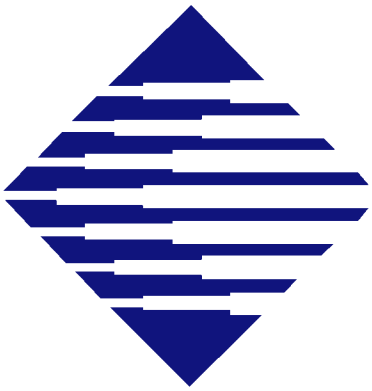
Warning:
Hazardous voltages are present. To reduce the risk of electrical shock and danger to personal health, follow the instructions.

Electrostatic Discharge



Caution:
Electronic components on printed circuit boards are extremely sensitive to static electricity. Ordinary amounts of static electricity generated by your clothing or work environment can damage the electronic equipment. It is recommended that anti-static ground straps and anti-static mats are used when installing the board in a system to help prevent damage due to electrostatic discharge.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Contents

Chapter 1: About This Guide 23

Overview 23
Related Documentation 25
Text Conventions 25
Customer Support and Services 26
Product Warranty 27

Chapter 2: Introduction 29

Overview 29
Product Description 29
Feature Summary 31
CPC4411 and CPC4416 Configurations 31
Applications 39
Additional Documentation 41
Free & Open Source Software 42

Chapter 3: Installation 45

Overview 45
Electrostatic Discharge 45
Slot/Shelf ID 46
DIP Switch and Jumper Options 46

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Backplane Connector Keys 55
Board Diagrams 57
Physical Installation 61
MAC Address Identification 61
Initial Setup 62

Chapter 4: Management 67

Overview 67
Front Panel LEDs 67
Command Line Interface (CLI) 69
Simple Network Management Protocol (SNMP) Agent 70
HTTP (Web) Server 70
Switch Security 70

Chapter 5: CLI Commands 73

Overview 73
Conventions 73
Entering Commands 75
Command Group Summary 78
Beacon Configuration 79
Manage BootP Settings 82
Manage Class of Service (COS) Settings 85
Console Port Settings 88
Date and Time 90
DHCP Client/Server Configuration 91
Event Manager 96
File System Management 100
File Transfer 106
Filter Mask Commands 110
Filtering Database 115
GARP (Generic Attribute Registration Protocol) Management 120

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

GMRP (GARP Multicast Registration Protocol) and Multicast Policy 122
GVRP (GARP VLAN Registration Protocol) Management 125
Command History 128
IGMP Snooping 129
Manage Internet Protocol (IP) Settings 132
Intelligent Platform Management Interface (IPMI): Field Replaceable Unit (FRU) 138
Intelligent Platform Management Interface (IPMI): Peripheral Management (PM) Controller . 149
Link Aggregation 152
Log Management 172
Network Diagnostics 175
Online Integrity Test Configuration 178
Password Management 180
Port Commands 181
Routing Management 186
Shell Commands 208
SNMP Configuration 211
Spanning Tree Management 225
Switch Management 237
Switch Security 241
Thresholds 247
User Login Name Management 249
VLAN Commands 250
Virtual Router Redundancy Protocol (VRRP) Management 254

Chapter 6: Simple Network Management Protocol 261

Overview 261
SNMP Agent Overview 261
Supported MIBs 262
Durable MIB Parameters 263
SNMP Trap Configuration 263
SNMP Version 3 265

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter 7: System Management Bus and Intelligent Platform Management 269

Overview . . . 269
Overview of SMB . . . 269
Intelligent Platform Management Interface (IPMI) . . . 270
Local IPMI Management . . . 272
System-Side IPMI Management . . . 272
IPM Device Commands . . . 274
FRU Inventory Device Commands . . . 280
Sensor/Event Commands . . . 285
OEM (Vendor Specific) Commands . . . 291

Chapter 8: Web Management 297

Overview . . . 297
HTTP Server Overview . . . 297

Chapter 9: Port Configuration 301

Overview . . . 301
Auto Polarity Sense and Auto MDX . . . 301
Port Configuration . . . 302

Chapter 10: VLANs 303

Overview . . . 303
GVRP . . . 304
VLAN Identification . . . 304
VLAN Management . . . 305
VLAN Configuration . . . 305

Chapter 11: Filtering Database 309

Overview . . . 309
Filtering Database Overview . . . 309

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Dynamic FDB Entries and Aging Timer . . . 309
Permanent FDB Entries . . . 310

Chapter 12: Packet Filtering 311

Overview . . . 311
Applications . . . 312
Operation . . . 312
Mask Table . . . 313
Rules Table . . . 314
Matching . . . 315
Using Egress and Ingress Port Masks . . . 315
Multiple Action Execution and Conflict Resolution . . . 315
Management Interfaces . . . 316
Filter Examples . . . 316

Chapter 13: Routing Protocols and IP Multihoming 325

Overview . . . 325
Routing (Layer3 Switching) . . . 325
Configuring Routing . . . 326
IP Multihoming . . . 331
RIP (Routing Information Protocol) . . . 334
OSPF (Open Shortest Path First) . . . 337

Chapter 14: Virtual Router Redundancy Protocol 357

Overview . . . 357
VRRP Overview . . . 357
Terminology . . . 358
Configuring the Simple VRRP Interface Router . . . 360
Load Sharing VRRP Interface Example . . . 363

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter 15: Spanning Tree 367

Overview . . . 367
Spanning Tree (STP) . . . 368
Fast Port . . . 369
Fast Uplink . . . 369
Port Path Cost . . . 372
Rapid Spanning Tree . . . 373
Differences Between RSTP and STP . . . 379
RSTP Configuration Example . . . 381

Chapter 16: Link Aggregation 385

Overview . . . 385
Link Aggregation Default Settings . . . 386
Architecture Overview . . . 388
Link Aggregation Configuration Examples . . . 394
Displaying Switch Configurations . . . 395

Chapter 17: Multicast Filtering 405

Overview . . . 405
Static Multicast Groups . . . 405
GMRP . . . 406
IGMP Snooping . . . 407

Chapter 18: DHCP Configuration 413

Overview . . . 413
Configuring the DHCP Server and Relay Agent . . . 414
DHCP and BootP Client . . . 422
DHCP Vendor Options . . . 422

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter 19: File System 425

Overview . . . 425
Remote File Systems . . . 426
Special Files . . . 427
Installing the CPC441x Application Software Image . . . 430
Upgrading the CPC441x Boot Files . . . 431
Board Application Software Recovery Procedure . . . 432
Configuring CPC441x Software . . . 440

Chapter 20: Diagnostic Tools 445

Overview . . . 445
Port Mirrors . . . 445
Ping . . . 446
Traceroute . . . 446
Embedded Diagnostics . . . 446
Fault State . . . 448

Chapter 21: Lua Programming Language 449

Overview . . . 449
Syntax . . . 450
Examples . . . 450
CPC441x Lua Library API . . . 470

Chapter 22: Specifications 487

Overview . . . 487
Electrical . . . 487
Mechanical . . . 488

Chapter 23: Rear Transition Modules & Board Pinouts 491

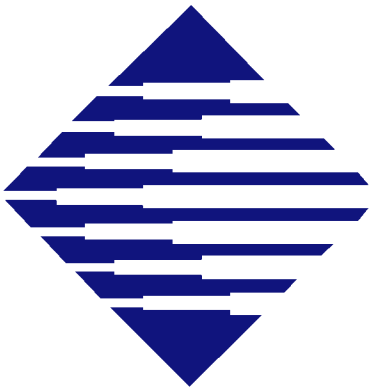
Overview . . . 491

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Rear Transition Modules 492
RTM Front Panel Diagrams 494
Port Pinouts 496
CPC4411 Main Board Pinouts 499
FlexLink™ Module 505
CPC4416 Main Board Pinouts 505

Index 515

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Tables

Table 2-1: Typical Applications - CPC4411 31

Table 2-2: Typical Applications - CPC4416 32

Table 3-1: SW3 Switch Settings 46

Table 3-2: SW1 Switch Settings 47

Table 3-3: Three-Pin Jumper Block Settings 47

Table 3-4: Four-Pin Jumper Block Settings 48

Table 3-5: SW7 Switch Settings 49

Table 3-6: SW6 Switch Settings 49

Table 3-7: Three Pin Jumper Block Settings (K9) 50

Table 3-8: Four Pin Jumper Block Settings (K10) 50

Table 3-9: Port 22 Mapping (SW3) 51

Table 3-10: Port 23 Mapping (SW4) 51

Table 3-11: Port 25 Mapping (SW1, 2) 52

Table 3-12: Port 26 Mapping (K1-8) 52

Table 3-13: Port 8 Configuration Switches (SW1) 53

Table 3-14: Fabric-to-Fabric SW1 Settings 54

Table 3-15: Shelf Geographic Address Switches (SW1, SW2) 55

Table 4-1: Port Link/Activity LED 68

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 4-2: Port Speed LED 68
Table 4-3: Port Speed LED 68
Table 4-4: System LED 68
Table 4-5: Fault LED 69
Table 5-1: Keywords for Interface Types 74
Table 5-2: Boolean Keywords 75
Table 5-3: Control-Key Commands for Line Editing 76
Table 5-4: Esc-Key Commands for Line Editing 77
Table 5-5: CLI Command Group Summary 78
Table 5-6: Event Names and Descriptions 96
Table 5-7: Basic ed Commands 104
Table 5-8: History Key-Commands 128
Table 5-9: Port Path Costs 226
Table 5-10: VLAN Display Legend 253
Table 6-1: Default SNMP Version 3 Users 266
Table 7-1: IPMB Slave Address Map 271
Table 7-2: Supported Network Function Codes 273
Table 7-3: IPM Device Request (Commands) Message Format 274
Table 7-4: IPM Device Response Message Format 275
Table 7-5: Get Device ID Response Message 276
Table 7-6: Set Manufacturing Test Mode ON Message Format 277
Table 7-7: Get Self Test Results Response Message 278
Table 7-8: Set ACPI Power State Request Message 278
Table 7-9: Get ACPI Power State Response Message 279
Table 7-10: Get Device GUID Response Message 279
Table 7-11: Broadcast Get Device IP Request Message 280

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-12: FRU Inventory Device Request Formats 281
Table 7-13: FRU Inventory Device Response Formats 281
Table 7-14: FRU Inventory Layout 282
Table 7-15: Get FRU Inventory Area Request Commands 282
Table 7-16: Get FRU Inventory Area Response Message 282
Table 7-17: Read FRU Inventory Data Request Commands 283
Table 7-18: Read FRU Inventory Data Response Message 283
Table 7-19: Write FRU Inventory Data Request Commands 284
Table 7-20: Write FRU Inventory Data Response Message 284
Table 7-21: Get Device SDR Info Request Message 285
Table 7-22: Get Device SDR Info Response Message 285
Table 7-23: Get Device SDR Request Message 286
Table 7-24: Get Device SDR Response Message 287
Table 7-25: Reserve Device SDR Repository Request Message 288
Table 7-26: Reserve Device SDR Repository Response Message 288
Table 7-27: SDR Type 0x11 - FRU Device Locator Record 289
Table 7-28: SDR Type 0x12 - Management Controller Device Locator Record 290
Table 7-29: Common OEM Request Commands 291
Table 7-30: Common OEM Response Commands 292
Table 7-31: Diagnostic Echo Request Commands 292
Table 7-32: Diagnostic Echo Response Message 292
Table 7-33: Bit Assignments for Card Power Status Byte 293
Table 7-34: Get Card Power Status Request Message 293
Table 7-35: Get Card Power Status Response Message 293
Table 7-36: Bit Assignments for Card Power State Byte 294
Table 7-37: Set Card Power State Request Message 294

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

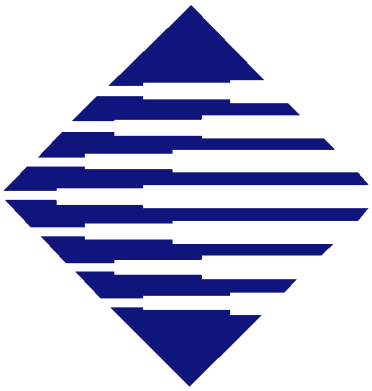
Table 7-38: Set Card Power State Response Message 295
Table 7-39: Get Card Power State Request Message 295
Table 7-40: Get Card Power State Response Message 295
Table 8-1: Web Pages and Descriptions 299
Table 12-1: Packet Filtering Mask Table 313
Table 12-2: Packet Filtering Rules Table. 314
Table 12-3: Packet Filtering Action Bits. 314
Table 12-4: Packet Key 317
Table 12-5: Packet Filtering Example 1: Mask Entry. 318
Table 12-6: Packet Filtering Example 1: Rule Entry 318
Table 12-7: Packet Filtering Example 2: Mask Entry. 320
Table 12-8: Packet Filtering Example 2: Rule Entry 320
Table 12-9: Packet Filtering Example 3: Mask Entry. 321
Table 12-10: Packet Filtering Example 3: Rule Entry 321
Table 12-11: Packet Filtering Example 4: Mask Entry. 322
Table 12-12: Packet Filtering Example 4: Rule Entry 323
Table 13-1: Hardware Tables 330
Table 13-2: OSPF General Parameters 337
Table 15-1: Port Path Costs 372
Table 15-2: STP and RSTP Port States 376
Table 17-1: IGMP PDU Processing. 409
Table 18-1: DHCP Configuration Types 417
Table 18-2: DHCP Configuration Parameters 418
Table 21-1: CPC441x Lua Programming Library. 470
Table 22-1: CPC4411 Power Consumption. 487
Table 22-2: CPC4416 Power Consumption. 488

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 22-3: CPC4411 Voltage Requirements 488
Table 22-4: CPC4416 Voltage Requirements 488
Table 23-1: CPC4411 and CPC4416 RTMs 492
Table 23-2: 10/100Mb Switched Ethernet Port Pinout. 496
Table 23-3: 1000Mb Switched Ethernet Port Pinout 496
Table 23-4: Ethernet Management Port Pinout 497
Table 23-5: RJ-11 Console Port Pinout 498
Table 23-6: DB-9 Console Cable Pinout 498
Table 23-7: CPC4411 Port Connections 499
Table 23-8: CPC4411 J1 Connector Pinout 500
Table 23-9: CPC4411 J2 Connector Pinout 501
Table 23-10: CPC4411 J3 Connector Pinout 502
Table 23-11: CPC4411 J4 Connector Pinout (Fabric Only). 503
Table 23-12: CPC4411 J5 Connector Pinout 504
Table 23-13: PTMC Port Mapping 505
Table 23-14: CPC4416 Port Connections 506
Table 23-15: CPC4416 J1 Connector Pinout 508
Table 23-16: CPC4416 J2 Connector Pinout 509
Table 23-17: CPC4416 (Node) J3 Connector Pinout 510
Table 23-18: CPC4416 (Fabric) J3 Connector Pinout 511
Table 23-19: CPC4416 J4 Connector Pinout - Fabric Only 512
Table 23-20: CPC4416 J5 Connector Pinout 514

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Figures

Figure 2-1: Redundant Fabric Boards in PICMG 2.16 Chassis 30

Figure 2-2: VoIP Media Gateway 40

Figure 2-3: Integrated Access Device (IAD) 40

Figure 2-4: IP DSLAM Device 41

Figure 2-5: Integrated Server Farm 41

Figure 3-1: CPC4411 Board Layout 57

Figure 3-2: CPC4411 Front Panel 58

Figure 3-3: CPC4416N Board Layout 59

Figure 3-4: CPC4416 Front Panels 60

Figure 7-1: CompactPCI SMB Block Diagram 271

Figure 8-1: Switch Configuration Web Page 298

Figure 10-1: Sample VLAN Configuration 307

Figure 13-1: IP Router 326

Figure 13-2: Sub-Networks with VLANs 327

Figure 13-3: Routing Configuration 328

Figure 13-4: Network 10.10.4.0 329

Figure 13-5: IP Multihoming on SW Interfaces 332

Figure 13-6: RIP Packet 335

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-7: RIP 2 Packet 336
Figure 13-8: Single Area Configuration 343
Figure 13-9: Multiple Area Configuration 348
Figure 13-10: Virtual Link Configuration 353
Figure 13-11: Stub Area 354
Figure 14-1: Simple Virtual Interface Router Example 359
Figure 14-2: Balanced Virtual Interface Router Example 365
Figure 15-1: Effect of Fast Port on Spanning Tree Convergence 369
Figure 15-2: Fast Uplink Before Direct Link Failure 370
Figure 15-3: Fast Uplink After Direct Link Failure 371
Figure 15-4: Loop-Free Topology 374
Figure 15-5: Port Roles 377
Figure 15-6: Alternate Port 378
Figure 15-7: Flag Fields for STP and RSTP 379
Figure 15-8: RSTP Configuration Example 381
Figure 16-1: CPC440x Architecture 389
Figure 16-2: CPC440x with Ports 1-3 Aggregated 391
Figure 16-3: Ports in Blocking State 392
Figure 16-4: Ports 1 - 3 Aggregated 393
Figure 16-5: Spanning Tree Configuration on Switch 1 395
Figure 16-6: Spanning Tree Configuration on Switch 2 396
Figure 16-7: Spanning Tree after Link Aggregation, Switch 1 398
Figure 16-8: Spanning Tree after Link Aggregation, Switch 2 399
Figure 16-9: LACP State Machines, Switch 1 400
Figure 16-10: LAC Port Information, Switch 1 401
Figure 16-11: LAC Aggregator Port Information, Switch 1 402

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 16-12: LAC Port Statistics, Switch 1 403

Figure 16-13: Link Aggregation Identifiers, Switch 1 404

Figure 19-1: Memory and Configuration Files 441

Figure 21-1: Redundant Ethernet Network Architecture 453

Figure 21-2: Automated Configuration Example 459

Figure 23-1: RTM Front Panel diagrams (1 of 2) 494

Figure 23-2: RTM Front Panel Diagrams (2 of 2) 495

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

1

About This Guide

Overview

This guide describes the CPC441x, Performance Technologies' fast, flexible Layer2/Layer3 Ethernet switching platform. Here's a brief description of what you'll find in this guide:

Here's a brief description of what you'll find in this guide:

Chapter 2, "Introduction" on page 29 contains a product description, model definitions and typical applications for the CPC441x and provides a framework for the rest of the document.

Chapter 3, "Installation," on page 45 covers the installation and initial setup of the CPC441x.

Chapter 4, "Management," on page 67 contains information regarding the front panel LEDs, the Command Line Interface (CLI), the SNMP agent, the HTTP server user interfaces, and security management.

Chapter 5, "CLI Commands," on page 73 describes the CPC441x Command Line Interface (CLI).

Chapter 6, "Simple Network Management Protocol," on page 261 describes the Simple Network Management Protocol (SNMP) agent implementation on the CPC441x.

Chapter 7, "System Management Bus and Intelligent Platform Management," on page 269 describes the Performance Technologies System Management Bus (SMB) and Intelligent Platform Management.

Chapter 8, "Web Management," on page 297 describes the HTTP Server-based management entity on the CPC441x.

Chapter 9, "Port Configuration," on page 301 contains information regarding configuring the CPC441x ports.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter 10, “VLANs,” on page 303 describes how the CPC441x Virtual LANS (VLANS) are configured and used.

Chapter 11, “Filtering Database,” on page 309 describes how the CPC441x Filtering Database entries are configured and used.

Chapter 12, “Packet Filtering,” on page 311 describes how CPC441x Packet Filtering Engine is configured and used.

Chapter 13, “Routing Protocols and IP Multihoming,” on page 325 provides an overview of routing as implemented on the CPC441x. It also describes IP Multihoming, and the two routing protocols supported by the CPC441x: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Chapter 14, “Virtual Router Redundancy Protocol,” on page 357 describes the Virtual Router Redundancy Protocol (VRRP).

Chapter 15, “Spanning Tree,” on page 367 contains information on configuring and using Spanning Tree on the CPC441x.

Chapter 16, “Link Aggregation,” on page 385 provides information about link aggregation on the CPC441x.

Chapter 17, “Multicast Filtering,” on page 405 describes static and dynamic multicast filtering on the CPC441x.

Chapter 18, “DHCP Configuration,” on page 413 discusses DHCP configuration on the CPC441x.

Chapter 19, “File System,” on page 425 describes the Flash file system that provides permanent storage for the CPC441x.

Chapter 20, “Diagnostic Tools,” on page 445 describes the diagnostic tools available to diagnose network problems on the CPC441x.

Chapter 21, “Lua Programming Language,” on page 449 describes the Lua Programming Language interface commands that allow customized operation of the CPC441x.

Chapter 22, “Specifications,” on page 487 describes the electrical and mechanical specifications for the CPC441x.

Chapter 23, “Rear Transition Modules & Board Pinouts,” on page 491 describes the rear transition modules, front panel diagrams, port pinouts, main board pinouts, and the FlexLink™ module.

An “Index,” on page 515 is also included.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Related Documentation

The following documentation is available from the PCI Industrial Computer Manufacturers' Group (http://www.picmg.org):

- *PICMG 2.16 CompactPCI® Packet Switching Backplane Specification Revision 1.0*
- *PICMG 2.9 CompactPCI® System Management Bus Specification Rev 1.0*
- *PICMG 2.0 CompactPCI® Specification Rev 3.0*

Text Conventions

This guide uses the following conventions:

Convention	What it is Used For
`Monospace font`	Monospace font is used to represent sample code.
Bold font	Bold font is used to represent: • pathnames • filenames • UNIX commands • user input
Italic font	Italic font is used to represent: • notes that supply useful advice • general information • referenced documents
$ARCH	Indicates the processor architecture of the target, currently this is ppc, mips, arm and i386.
$\overline{\text{Overline}}$	An overline is used to represent an Active Low signal.
< >	Angle brackets are used to represent variables (for example, file names, passwords).
ALL CAPITALS	All capital letters are used for the keys on your keyboard (for example, the ENTER, the TAB, and the SPACEBAR keys).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Customer Support and Services

Performance Technologies offers a variety of standard and custom support packages to ensure customers have access to the critical resources that they need to protect and maximize hardware and software investments throughout the development, integration, and deployment phases of the product life cycle.

If you encounter difficulty in using this Performance Technologies, Inc. product, you may contact our support personnel by:

1. **EMAIL** (Preferred Method) – Email us at the addresses listed below or use our online email support form. Outline your problem in detail. Please include your return email address and a telephone number.
2. **TELEPHONE** – Contact us via telephone at the number listed below, and request Technical Support. Our offices are open Monday to Friday, 8:00 a.m. to 8:00 p.m. (Eastern Standard Time).

	Embedded Systems and Software (Includes Platforms, Blades, and Servers)	SS7 Systems (Includes SEGway™)
Email	support@pt.com	ss7support@pt.com
Phone	+1 (585) 256-0248 (Monday to Friday, 8 a.m. to 8 p.m. Eastern Standard Time)	+1 (585) 256-0248 (Monday to Friday, 8 a.m. to 8 p.m. Eastern Standard Time)

If you are located outside North America, we encourage you to contact the local Performance Technologies' distributor or agent for support. Many of our distributors or agents maintain technical support staffs.

Customer Support Packages

Our configurable development and integration support packages help customers maximize engineering efforts and achieve time-to-market goals. To find out more about our Customer Support packages, visit http://www.pt.com/page/support/.

Other Web Support

Support for existing products including manuals, release notes, and drivers can be found on specific product pages at http://www.pt.com. Use the product search to locate the information you need.

Return Merchandise Authorization (RMA)

To submit a return merchandise authorization (RMA) request, complete the online RMA form available at http://pt.com/assets/lib/files/rma-request-form.doc and follow the instructions on the form. You will be notified with an RMA number once your return request is approved. Shipping information for returning the unit to Performance Technologies will be provided once the RMA is issued.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

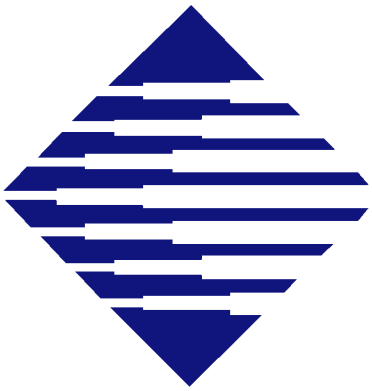
Product Warranty

Performance Technologies, Incorporated, warrants that its products sold hereunder will at the time of shipment be free from defects in material and workmanship and will conform to Performance Technologies' applicable specifications or, if appropriate, to Buyer's specifications accepted by Performance Technologies in writing. If products sold hereunder are not as warranted, Performance Technologies shall, at its option, refund the purchase price, repair, or replace the product provided proof of purchase and written notice of nonconformance are received by Performance Technologies within 12 months of shipment, or in the case of software and integrated circuits within ninety (90) days of shipment and provided said nonconforming products are returned F.O.B. to Performance Technologies's facility no later than thirty days after the warranty period expires. Products returned under warranty claims must be accompanied by an approved Return Material Authorization number issued by Performance Technologies and a statement of the reason for the return. Please contact Performance Technologies, or its agent, with the product serial number to obtain an RMA number. If Performance Technologies determines that the products are not defective, Buyer shall pay Performance Technologies all costs of handling and transportation. This warranty shall not apply to any products Performance Technologies determines to have been subject to testing for other than specified electrical characteristics or to operating and/or environmental conditions in excess of the maximum values established in applicable specifications, or have been subject to mishandling, misuse, static discharge, neglect, improper testing, repair, alteration, parts removal, damage, assembly or processing that alters the physical or electrical properties. This warranty excludes all cost of shipping, customs clearance and related charges outside the United States. Products containing batteries are warranted as above excluding batteries.

THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS. IN NO EVENT SHALL PERFORMANCE TECHNOLOGIES BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES DUE TO BREACH OF THIS WARRANTY OR ANY OTHER OBLIGATION UNDER THIS ORDER OR CONTRACT.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Chapter

2

Introduction

Overview

This chapter contains a product description, model definitions and typical applications of the CPC441x. The key topics in this chapter include:

- “Product Description” on page 29
- “Feature Summary” on page 31
- “CPC4411 and CPC4416 Configurations” on page 31
- “Applications” on page 39
- “Additional Documentation” on page 41
- “Free & Open Source Software” on page 42

Product Description

The CPC4411 and CPC4416 are robust, flexible, full wire-speed Layer2/Layer3 Ethernet switches that are compatible with both PICMG 2.16 and non-2.16 backplanes. The CPC4411 features 24 10/100 auto-negotiating ports plus two gigabit fiber uplinks. The CPC4416 provides 24 10/100 ports plus two gigabit TX ports. In addition, the CPC4416 features a FlexLink PTMC site, which allows the integration of a variety of co-processor, network processor, or front panel breakout options, including up to four additional Ethernet ports; of which two can be gigabit ports.

The CPC4411 and CPC4416 provide developers of server clusters, wireless, IP telephony, public safety and broadband access systems the ideal solution for applications requiring high availability, increased bandwidth, performance and reliability.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

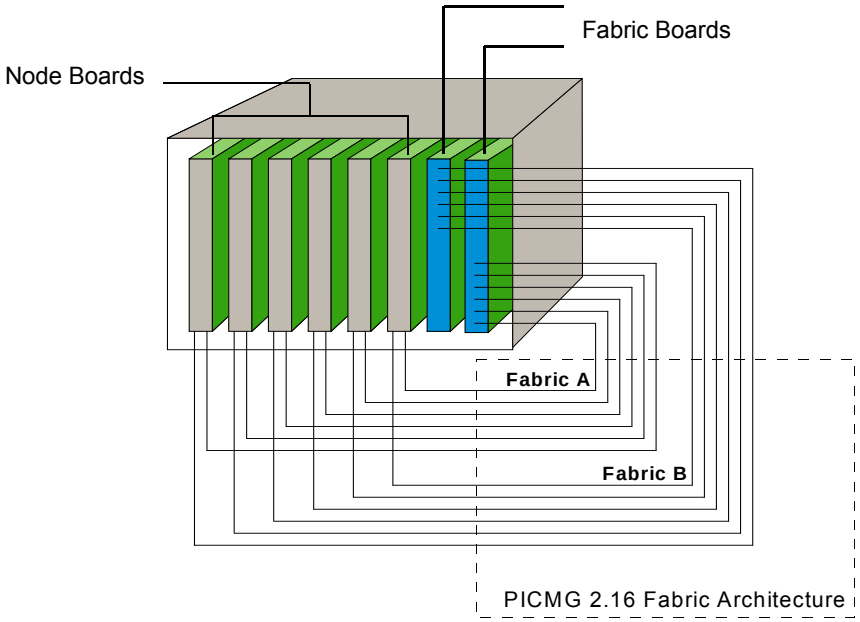
CompactPCI Packet Switching Backplane (CompactPCI/PSB)

The PICMG 2.16 specification defines the CompactPCI Packet Switching Backplane. Performance Technologies' products are compliant with this standard, which offers the option of sending all Ethernet signals through the backplane. By moving system traffic from the shared bus architecture to a fault-tolerant switched backplane, overall system throughput can be vastly increased while retaining the reliability and hot-swap capacity of CompactPCI.

A PICMG 2.16 compliant system accommodates Fabric boards and Node boards.

- A **Fabric** board links to each Node board in a packet switching chassis. In this way, every Node board can communicate with every other Node board, thereby forming a switching fabric. In redundant configurations using two Fabric boards, the Fabric boards can be linked to each other. A Fabric board can only be used in a Fabric slot.
- A **Node** board links to the Fabric board in a PICMG 2.16 compliant chassis. In redundant configurations using two Fabric boards, each Node board is linked to both Fabric boards. Node boards can only be used in Node slots.

Figure 2-1: Redundant Fabric Boards in PICMG 2.16 Chassis



As shown above, each of the two Fabric slots is independently connected to each of the Node slots.

Please refer to the PICMG 2.16 specification and the supporting documentation for your chassis for more information on configuring a packet switching backplane.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Feature Summary

- CPC4416: Twenty-four 10/100Mbs plus two 10/100/1000Mbs Ethernet ports.
- CPC4411: Twenty-four 10/100Mbs plus two fiber gigabit ports.
- FlexLink™ PTMC Type 5 slot on CPC4416 for NAT/LSNAT, IP Tunneling, or front panel uplinks.
- Front panel 10/100Mbps out-of-band Ethernet port for management.
- Full duplex, full wire speed Layer3 switching (IPv4) at all Ethernet frame sizes.
- Support for hardware connection layer of PICMG 2.1 Hot Swap.
- Support for PICMG 2.9/IPMI v1.5 System Management Bus (SMB).
- 8K MAC addresses.
- 802.1p priority queuing (4 classes of service per egress port).
- 802.1Q VLAN support (up to 4K VLANs).
- 802.3-2000 Link Aggregation (up to 6 groups, 8 ports per group).
- Front or rear panel console port (RS-232).
- CLI management interface with scripting language for value-added applications.
- SNMP v1, v2c, v3.
- 32 Mbyte Flash-based file system on CPC4416; 8 Mb on CPC4411.
- Front panel LEDs indicating system status, link, speed, and activity.
- Power-On or management (CLI or SNMP) invoked diagnostics.
- RTM module options for rear panel I/O of switched Ethernet ports.
- Locking ejector handles on CPC441x main board and RTMs.

CPC4411 and CPC4416 Configurations

The CPC4411 and CPC4416 platforms support a variety of configurations. With the use of Rear Transition Modules (RTMs), the customer may select how many unused CompactPCI/PSB Link Ports are brought out as Ethernet ports for external connectivity. Typical embedded applications will have most Ethernet ports connected within the midplane. Both switches can also be used as an enterprise solution in which most Ethernet ports are connected externally to the chassis. The following tables identify several possible configurations:

Table 2-1: Typical Applications - CPC4411

Application	10/100Base-T ports on mid-plane	10/100Base-T ports on RTM
PICMG 2.16 Standard Fabric Slot	19	5 RJ-45
PICMG 2.16 Extended Fabric Slot	24	0
Enterprise Application	0	24 RJ-45
Enterprise Application	0	24 RJ-45 Dual RJ-21 with Patch Panel

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 2-2: Typical Applications - CPC4416

Application	100Base-T ports on mid-plane	100Base-T ports on RTM	1000Base-T ports on RTM	LPf (fabric to fabric) Support	PTMC Ethernet ports
PICMG 2.16 Standard Fabric Slot (no PTMC)	19	4	2	Y	0
PICMG 2.16 Standard Fabric Slot (1 port gig PTMC)	19	4	1	Y	1
PICMG 2.16 Standard Fabric Slot (4 port PTMC)	19	2	0	Y	4
PICMG 2.16 Extended Fabric Slot	24	0	0	N	0
PICMG 2.16 Node Slot	2 (1000Mb)	24	0	NA	0
Enterprise Application	0	24	2	NA	0
Enterprise Application (1 port PTMC)	0	24	1	NA	1
Enterprise Application (4 port PTMC)	0	22	0	NA	4

PCI Bus

The CPC441x operates independent of the PCI bus. As an option, the CPC441x supports the CompactPCI bus as a routed bus on the J1 connector, using the following PCI signals:

- $\overline{\text{RST}}$
- $\overline{\text{BDSEL}}$
- $\overline{\text{HEALTHY}}$

Switched Ethernet Ports

The CPC441x provides (24) 10/100Mb Ethernet ports and (2) 1000Mb Ethernet ports interconnected via a fully meshed 9 Gbps switching fabric. An 802.1D bridge relay entity exists between any pair of switched ports. The switched Ethernet ports offer low latency, wire-speed, Layer 2/3 switching performance on all ports simultaneously. The CPC441x supports 8191 (8K) MAC Address entries (simultaneously) in its filtering database.

The CPC441x provides a logical link control (LLC) interface between the IP Stack of the embedded onboard operating system and the switched ports. This interface allows for sending and receiving frames to/from the onboard CPU and any of the switched Ethernet ports. This capability allows the onboard CPU to be a presence on the attached network and allows external clients to manage the operation of the switch via any of the switched Ethernet ports.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Out-of-Band (Management) Ethernet Port

One 10Base-T/100Base-TX non-switched Ethernet port is provided on the CPC441x for switch management purposes. This port conforms to all requirements of the IEEE 802.3 (CSMA/CD) MAC interface.

This port does *not* have a MAC Relay Entity between itself and any of the switched Ethernet ports. This separation makes it possible to allocate all switched ports to users while always maintaining a secure and available path to manage the switch.

The CPC441x provides an LLC interface between the IP stack of the embedded onboard operating system and the out-of-band Ethernet port. This interface allows sending and receiving frames to and from the onboard CPU and the out-of-band Ethernet port. This capability allows the onboard CPU to be a presence on the attached network and allows external clients to manage the operation of the switch via the out-of-band Ethernet port.

The out-of-band Management port provides access to a separate subnet from that of the switched ports. The CPC441x must be provided with an IP address for each LLC Interface that is to be enabled. If the out-of-band Ethernet interface is to be used, it must be assigned an IP address and subnet mask combination that place the interface in a separate subnet from that of the switched ports.

Spanning Tree and Rapid Spanning Tree

The CPC441x supports both Spanning Tree (IEEE 802.1D-1998), and Rapid Spanning Tree (802.1D-2004). Both link management protocols provide path redundancy while preventing loops in a network, but they differ in operation. RSTP can interoperate with both STP and RSTP devices, but when RSTP operates in STP-compatible mode, it behaves like STP but does not run STP code. (See Chapter 15, “Spanning Tree,” on page 367.)

Spanning Tree Extensions

The CPC441x supports a pair of extensions to the standard Spanning Tree protocol that enhance its utility in building fault tolerant networks. The standard Spanning Tree protocol supports redundant links for resiliency, but the algorithm that selects the active link can take anywhere from 30 to 50 seconds to converge. This delay often causes Application layer timeouts. The CPC441x addresses this problem with two extensions to the Spanning Tree protocol: Fast Uplink and Fast Port.

Fast Uplink

Fast Uplink allows a redundant pathway toward the Root Bridge to be quickly selected upon failure of link integrity on the current path to the Root Bridge. The switch-over time is typically less than 1 second. (See “Fast Uplink” on page 369.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Fast Port

Fast Port allows the user to select ports that do not need to participate in the Spanning Tree protocol. These ports must have simple client stations attached to them and must not provide a path to any device that might act as a bridge between LAN segments. That is, the user must ensure that no bridges or routers can be accessed through a port that has Fast Port turned on. When Fast Port is turned on, the port will not participate in Spanning Tree and will not undergo or cause any Spanning Tree topology changes. (See “Fast Port” on page 369.)

VLANs

The CPC441x provides support for Virtual LANs (VLANs) which allows you to construct broadcast domains without being restricted by physical connections. Up to 16 VLANs can be defined on the CPC441x. A VLAN is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN). Implementing VLANs on your network has the following advantages:

- VLANs control broadcast traffic. If a device in a particular VLAN transmits a broadcast frame, only devices in that VLAN receive the frame.
- VLANs provide extra security. Devices in a VLAN can only communicate with devices on the same VLAN.
- VLANs ease moves, adds, and changes of devices on networks. If a device in a VLAN is moved to a port in another part of the network, simply configure the new port to be in the VLAN of the moved device.
- If the end node device is VLAN aware, the port will automatically forward the packets to the proper location. No reconfiguration is required.

See Chapter 10, “VLANs,” on page 303.

Port Mirroring

Port Mirroring allows the user to monitor the traffic on any port with an analyzer connected to the “mirrored-to” port. The CPC441x offers the ability to monitor frames transmitted to a port, received from a port, or both.

This feature is a very useful tool for network administrators to detect and correct network malfunctions, or for developers to aid in debugging network applications and protocols. See Chapter 20, “Diagnostic Tools,” on page 445.

Multicast Filtering Mechanisms

The CPC441x supports static and dynamic multicast filtering. Multicast filtering allows the user to restrict the propagation of frames destined for a group of recipients to only those ports that provide a path to devices in that group.

Dynamic Multicast MAC Registration

Dynamic Multicast MAC Registration is supported via GMRP (GARP Multicast Registration Protocol) and IGMP Snooping.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

GMRP Registration

Through the operation of the GMRP protocol, stations that are interested in being members of a multicast group make registration requests. The switch dynamically maintains a list of the member ports and only sends multicast frames to those ports that have members. This frees up bandwidth on those ports that have no members in a group. The switch also announces to other inter-networking devices that support GMRP, that the switch is a pathway to member stations. This allows member stations to “find” each other across a bridged LAN.

Multilcast Filtering and IGMP Snooping

IGMP (Internet Group Management Protocol) Snooping allows the switch to forward multicast traffic intelligently. By monitoring the IGMP query and report messages (“snooping”), the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance. The switch may also be configured to send periodic query messages to allow for Layer-2 IGMP operation without the presence of a multicast router. (See Chapter 17, “Multicast Filtering,” on page 405.)

Broadcast Storm Suppression

The CPC441x offers the ability to limit forwarding of Broadcasts, Multicasts, and frames with unknown Destination MAC Addresses (flooding). The user can set a maximum frame rate forwarded by the switch for these traffic types. This feature prevents malfunctioning network equipment from flooding the network.

Quality/Class of Service (COS)

The CPC441x supports four traffic priority queues per egress port. Each queue provides a different class of service, i.e., those frames queued to the higher priority queues are transmitted ahead of those on the lower priority queues.

The CPC441x assigns frames to the egress port queues on the basis of the priority field carried with the 802.1Q tag header, or based on packet filters. The 802.1Q specification allows for 8 traffic classes to be specified in the tag header field of the frame. The 8 traffic classes are mapped to the 4 available COS Queues. The mapping is programmable.

Once packets have been mapped to the four COS queues, the queues are drained at the egress port based on a programmable scheduling algorithm. The possible scheduling algorithms include: Strict Priority, Weighted Round Robin, and Weighted Round Robin with Bounded Delay. (See “Manage Class of Service (COS) Settings” on page 85.)

Packet Filtering

The CPC441x supports a packet classification and filtering mechanism that allows the user to define special handling actions for packets based on the content of the first 80 bytes of the packet.

Typical applications for Packet Filtering include:

- Traffic Prioritization
- Firewall Creation

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- Bandwidth Regulation
- Network Monitoring and Troubleshooting

See Chapter 12, “Packet Filtering,” on page 311.

CPC441x Embedded Diagnostics

The embedded diagnostic functions of the CPC441x ensure virtually faultless operation both at initialization and continuously during switch operation. The In-System verification includes Power-On Confidence (POC) tests and Online Integrity tests.

Power-On Confidence (POC) Tests

Power-On Confidence (POC) tests are diagnostic tests run when the CPC441x is booted. The POC test suite includes only those diagnostic tests that do not affect externally attached devices. When running POC tests, the CPC441x becomes available to the user within 60 seconds of a power-on or reset. All subsystems are included in the POC suite.

Online Integrity Tests

These are tests that are run on a continuous basis while the CPC441x is in service. Online Integrity Tests are enabled by default, but the CPC441x also provides a method to disable them.

The integrity tests continuously operate during execution of application code to detect hardware faults. Upon detecting a fault, the CPC441x can take itself out of service. All attached clients will lose link. (See “Online Integrity Test Configuration” on page 178.)

Watchdog Timer

A hardware watchdog timer is supported that will remove the CPC441x from service if it is not refreshed periodically by the CPU. This guards against CPU failure. If the watchdog timer expires, link will be deasserted on all external ports, and the CPC441x will be reset. The user can configure the board to reboot after a watchdog event or to remain off line.

Network Services

The CPC441x provides network services to attached clients, thus avoiding the need for an expensive server in some embedded applications. Services offered include: File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP), access to the Flash-based file system, and Dynamic Host Configuration Protocol (DHCP) IP Address allocation services.

FTP/TFTP Server

The CPC441x offers an on-board Flash-based file system. The file system is available to attached Ethernet clients and allows them to store and retrieve configuration files using FTP or TFTP.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

DHCP and BootP Server

The CPC441x provides a basic set of DHCP (Dynamic Host Configuration Protocol) services to attached clients. The DHCP server is capable of supplying IP addresses to clients. IP Addresses are provided based upon one of three keys: MAC Address, Port, or Client ID. See “Configuring the DHCP Server and Relay Agent” on page 414.

Management Interfaces

The CPC441x provides three management interfaces to the user: Command Line Interface (CLI), Simple Network Management Protocol (SNMP), and the World Wide Web (HTTP).

Command Line Interface (CLI)

The CLI is available to the user through the RS-232 console port of the CPC441x or via Telnet after the CPC441x has been configured for network operation. The CPC441x CLI functions as:

- An initial configuration interface
- A simple and efficient management user interface
- A command interpreter for scripting
- A debugging tool for development and testing

See “Command Line Interface (CLI)” on page 69 and Chapter 5, “CLI Commands,” on page 73 for details.

SNMP

The CPC441x SNMP agent allows for management of the CPC441x through a remote SNMPv1/v2c/v3 client application. The agent responds to a defined set of SNMP client requests and generates the appropriate SNMP traps to respond to CPC441x events. See “SNMP Configuration” on page 211 and “SNMP Agent Overview” on page 261.

HTTP

The CPC441x provides a management interface through an onboard web server. After setting an IP address, point your browser at the IP Address of the CPC441x to manage the CPC441x through this interface. See Chapter 8, “Web Management,” on page 297 for more information.

Programming Interface

The CPC441x provides a programming language interface that allows customized operation of the switch. This language is based on the Lua programming language designed and implemented at TeCGraf, the Computer Graphics Technology Group of PUC-Rio (the Pontifical Catholic University of Rio de Janeiro in Brazil). TeCGraf is a laboratory of the Department of Computer Science.

The CPC441x incorporates Lua as the language of customer provided application programs. Application programs are files written in Lua that allow the user to detect events, inspect status, and modify switch configuration. For more information, see Chapter 21, “Lua Programming Language,” on page 449.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Layer 3 Routing

The CPC441x is a “Layer 2/3” switch, which means that it combines the speed of Layer 2 switching with the intelligence of Layer 3 routing. By examining Layer3 data in hardware, the CPC441x is able to route Layer3 traffic at wire speed.

Virtual Router Redundancy Protocol (VRRP)

VRRP makes it possible for multiple switches to be configured as a single virtual router, providing redundant data paths and thereby eliminating the single point of failure in a network. The router associated with a given alternate path supported by VRRP uses the same IP address and MAC address as the routers for other paths. As a result, the host’s gateway information does not change, no matter what path is used. Because of this, VRRP-based redundancy significantly reduces administrative overhead when compared to redundancy schemes that require hosts to be configured with multiple default gateways. See Chapter 14, “Virtual Router Redundancy Protocol,” on page 357.

Routing Protocols

The CPC441x supports two routing protocols: RIP (Routing Information Protocol), and OSPF (Open Shortest Path First). RIP is a distance-vector protocol that uses hop count as its metric. It is an *interior gateway protocol* (IGP), which means that it performs routing within a single autonomous system. The latest enhancement to RIP is the RIP2 specification, which allows more information to be included in RIP packets and provides a simple authentication mechanism. The CPC441x supports both RIP and RIP2.

OSPF is a link-state protocol that builds a complete picture of a network and finds the shortest path to a destination based on the algorithm employed. Unlike RIP, OSPF is well-suited for large networks.

Using a two-tier topology, OSPF supports the formation of “areas,” which are contiguous portions of a network within an autonomous system. Each area uses a separate topology database and is invisible to all other areas. This makes it possible for OSPF to minimize the amount of routing traffic. See Chapter 13, “Routing Protocols and IP Multihoming,” on page 325.

System Management Bus (PICMG 2.9)

The CPC441x includes the Performance Technologies implementation of the System Management Bus (SMB). This conforms to PICMG 2.9, the specification that defines SMB in the CompactPCI environment. SMB utilizes the I^2C bus hardware layer coupled with Intelligent Platform Management software. The Intelligent Platform Management Interface specification allows system components on the I^2C hardware layer bus to communicate with each other, thereby making possible “out of band” management of a system’s resources, with an emphasis on controlling hot-swap activities. See Chapter 7, “System Management Bus and Intelligent Platform Management,” on page 269.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Link Aggregation

Link Aggregation allows up to eight physical ports to be aggregated together, forming a Link Aggregation Group. This aggregation can then function as if it were a single link, which means that constituent links that would otherwise be blocked as redundant by Spanning Tree can continue providing increased link capacity. Link Aggregation also provides higher link availability, since the loss of an individual port will not disrupt communication. See Chapter 16, “Link Aggregation,” on page 385.

Beacon Protocol

The Beacon Protocol invokes a signal that informs a host that the switch is running, and that it has network connectivity. The switch will send beacon messages using a specified interface to a destination address/UDP port at the specified interval. Using an IP multicast address as the destination (e.g. 224.1.2.3) allows all interested hosts to receive the beacon messages while not placing a burden on other hosts. For those hosts unable to process IP multicast packets, individual beacons can be created.

Secure Shell (SSHv2)

Secure Shell protocol provides secure encrypted communication between untrusted hosts over an insecure network. It is designed to replace inherently insecure communication protocols such as Telnet. SSHv2 provides secure remote logins, while effectively eliminating eavesdropping, connection hijacking and other network attacks. SSHv2 supports the DSA, SHA-1, Blowfish, and 3-DES cryptographic algorithms.

Applications

Due to its stand-alone architecture and CompactPCI chassis compatibility, the CPC441x is suitable for integration into many types of high-availability (HA) as well as non-HA Ethernet switching applications. These applications include:

- VoIP Media Gateway
- Integrated Access Devices (IAD)
- IP DSLAM Architecture
- Integrated Server Farms

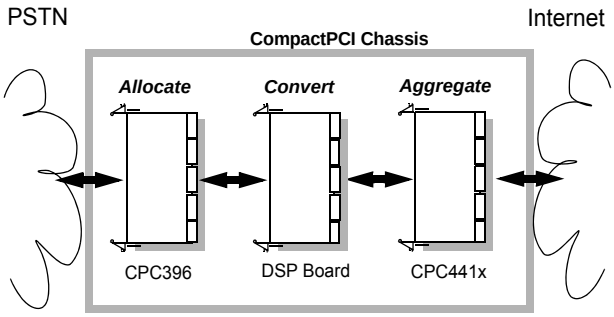
Voice-Over-IP Media Gateway

The Voice-over-IP media gateway application consists of three major functional blocks. The Allocate, Convert, and Aggregate blocks make up the simplified bridge architecture between traditional PSTN voice circuits and the Internet.

Figure 2-2: “VoIP Media Gateway” on page 40 shows a block diagram of a simplified media gateway. In this example, the Allocate function allocates circuits from the PSTN through a TDM switch to H.110-based DSPs. The DSPs serve to convert the PSTN circuit into IP frames. The IP frames are collected and aggregated into a high speed Ethernet uplink to be sent over the Internet. Another Performance Technologies product, the CPC396 Dual Channel T3/H.110 TDM Switch provides the allocation function in this example.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

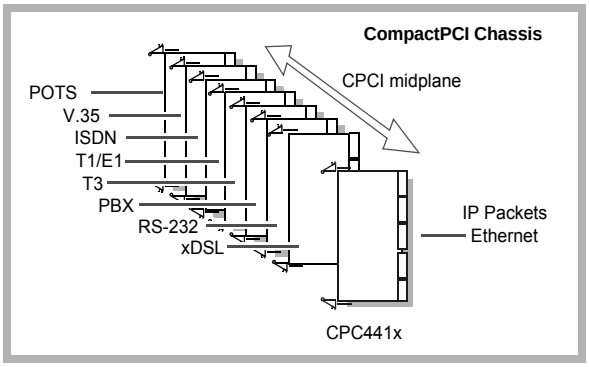
Figure 2-2: VoIP Media Gateway



Integrated Access Device (IAD)

The Integrated Access Device consists of a gathering of different types of digital and analog interface boards that are commonly tied together through the CompactPCI midplane. The CPC441x provides a common Ethernet interface for the assortment of devices. See Figure 2-3: “Integrated Access Device (IAD)” on page 40.

Figure 2-3: Integrated Access Device (IAD)

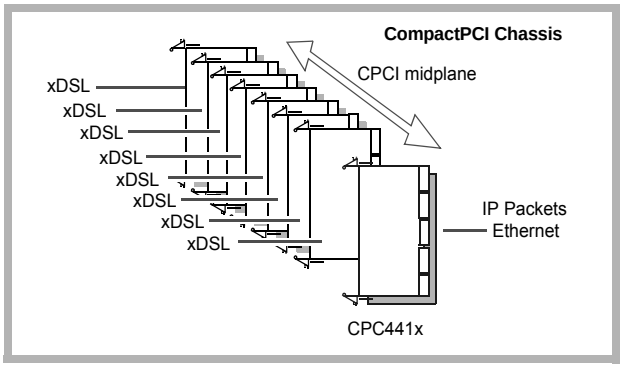


IP DSLAM Device

The IP DSLAM (Digital Subscriber Line Access Multiplexer) device concentrates multiple xDSL interfaces onto an IP packet Ethernet interface. See Figure 2-4: “IP DSLAM Device” on page 41. The CPC441x aggregates the traffic from multiple xDSL line interface cards onto gigabit uplinks for transmission over the Internet.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

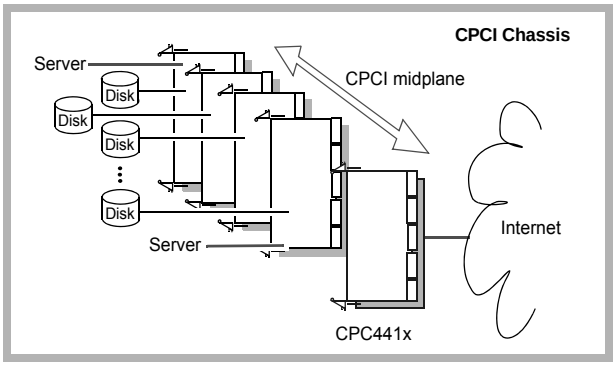
Figure 2-4: IP DSLAM Device



Integrated Server Farm

The Integrated Server Farm collapses an entire network of servers into a single chassis. See Figure 2-5: “Integrated Server Farm”. The CompactPCI chassis is populated with servers attached to their file systems (disks). The CPC441x provides inter-connectivity between the servers as well as gigabit uplinks to the Internet.

Figure 2-5: Integrated Server Farm



Additional Documentation

The following documentation is available from the PCI Industrial Computer Manufacturers’ Group (http://www.picmg.org):

- *PICMG 2.16 CompactPCI® Packet Switching Backplane Specification Revision 1.0*
- *PICMG 2.9 CompactPCI® System Management Bus Specification Rev 1.0*
- *PICMG 2.0 CompactPCI® Specification Rev 3.0*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Free & Open Source Software

This section contains the wording of the license agreements for all Free & Open Source Software (FOSS). We currently utilize two software packages of this type. One is LUA, which is used for our Command Line Interpreter (CLI) and the other is traceroute which is used for our `traceroute` command.

LUA License Agreement

The following is the License for LUA (taken from the source):

```
/******************************************************************************
* Copyright (C) 1994-2000 TeCGraf, PUC-Rio. All rights reserved.
*
* Permission is hereby granted, without written agreement and without license
* or royalty fees, to use, copy, modify, and distribute this software and its
* documentation for any purpose, including commercial applications, subject to
* the following conditions:
*
*  - The above copyright notice and this permission notice shall appear in all
*    copies or substantial portions of this software.
*
*  - The origin of this software must not be misrepresented; you must not
*    claim that you wrote the original software. If you use this software in a
*    product, an acknowledgment in the product documentation would be greatly
*    appreciated (but it is not required).
*
*  - Altered source versions must be plainly marked as such, and must not be
*    misrepresented as being the original software.
*
* The authors specifically disclaim any warranties, including, but not limited
* to, the implied warranties of merchantability and fitness for a particular
* purpose. The software provided hereunder is on an “as is” basis, and the
* authors have no obligation to provide maintenance, support, updates,
* enhancements, or modifications. In no event shall TeCGraf, PUC-Rio, or the
* authors be held liable to any party for direct, indirect, special,
* incidental, or consequential damages arising out of the use of this software
* and its documentation.
*
* The Lua language and this implementation have been entirely designed and
* written by Waldemar Celes Filho, Roberto Ierusalimschy and
* Luiz Henrique de Figueiredo at TeCGraf, PUC-Rio.
*
* This implementation contains no third-party code.
******************************************************************************/
```

traceroute License Agreement

The following is the License for traceroute (taken from the source):

```
/*
 * Copyright (c) 1988, 1989, 1991, 1994, 1995, 1996, 1997
 *  The Regents of the University of California. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
* modification, are permitted provided that: (1) source code distributions
* retain the above copyright notice and this paragraph in its entirety, (2)
* distributions including binary code include the above copyright notice and
* this paragraph in its entirety in the documentation or other materials
* provided with the distribution, and (3) all advertising materials mentioning
* features or use of this software display the following acknowledgement:
* ``This product includes software developed by the University of California,
* Lawrence Berkeley Laboratory and its contributors.'' Neither the name of
* the University nor the names of its contributors may be used to endorse
* or promote products derived from this software without specific prior
* written permission.
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED
* WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
* MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
*/
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

3

Installation

Overview

This section covers the installation and initial setup of the CPC441x. The key topics in this chapter include:

- “Electrostatic Discharge” on page 45
- “Slot/Shelf ID” on page 46
- “DIP Switch and Jumper Options” on page 46
- “Backplane Connector Keys” on page 55
- “Board Diagrams” on page 57
- “Physical Installation” on page 61
- “MAC Address Identification” on page 61
- “Initial Setup” on page 62

Electrostatic Discharge

Caution:
Electronic components on printed circuit boards are extremely sensitive to static electricity. Ordinary amounts of static electricity generated by your clothing or work environment can damage the electronic equipment. When installing the board in a system, you must use anti-static grounding straps and anti-static mats to prevent damage due to electrostatic discharge.

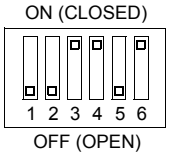
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Slot/Shelf ID

The CPC441x provides access to the Slot ID for both Node and Fabric applications, and to the Shelf ID for Fabric applications. Both of these are provided via the private enterprise MIB. This allows SNMP applications and Lua scripts access to this information.

DIP Switch and Jumper Options

The DIP switch and jumper settings available on the CPC4411 and CPC4416 are shown in the following tables. An asterisk (*) indicates the factory default setting.



Note: *Each DIP microswitch is ON (closed) in the up position, and OFF (open) in the down position.*

CPC4411 Switch and Jumper Settings

Table 3-1: SW3 Switch Settings

DIP Switch	Description	OFF	ON
1	Reserved	* Disabled	Enabled
2	SMB Enable	Disabled	* Enabled
3	SMB_BDSEL - connects CompactPCI BDSEL to the SMB controller.	Disabled	* Enabled
4	RST_SMB - enables the SMB Controller to assert switch reset.	Disabled	* Enabled

* = factory default

When the **SMB Enable** switch is closed, the SMB controller is enabled. When this switch is open, the SMB controller is disabled. The SMB controller will not respond to commands unless it is enabled.

When **SMB_BDSEL** is ON (closed) the SMB controller can monitor the PCI bus **BDSEL#** signal. When OFF (open), **BDSEL#** is isolated from SMB. The SMB controller will wait for up to two seconds for BDSEL# to be asserted after power-on before it attempts to acquire the Geographical Address from the backplane and complete its initialization. If **BDSEL#** is not asserted within two seconds, the SMB controller continues its initialization.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

When **RST_SMB** switch is ON (closed), the SMB controller can reset the switch when it receives an IPMI command to do so. See Chapter 7, “System Management Bus and Intelligent Platform Management,” on page 269. When OFF (open), on-board reset is isolated from the SMB controller. Other sources of reset are independent of this setting, such as PCI Reset, Push Button Reset, etc.

Table 3-2: SW1 Switch Settings

DIP Switch	Description	OFF	ON
1	Burn-In Mode (ESS)	* Disabled	Enabled
2	User Defined Bit 3 (UDJ3 in SCR)	Set (1)	* Cleared (0)
3	User Defined Bit 2 (UDJ2 in SCR)	Set (1)	* Cleared (0)
4	User Defined Bit 1 (UDJ1 in SCR)	Set (1)	* Cleared (0)
5	PCI Reset	* Disabled	Enabled
6	Break Detect	* Disabled	Enabled

* = factory default

The **ESS** function is used only at the factory to burn-in boards and should not be moved by the user.

The status of **User Defined** signals is available via an enterprise MIB variable which is accessible from the CLI and SNMP.

The PCI Reset switch connects the on-board reset to the PCI Reset signal. This allows the switch to be reset or not when the CompactPCI bus is reset.

The **Break Detect** switch allows the user to generate a hard reset on the board by sending a BREAK signal in through the console port. This is a useful remote debugging feature.

Table 3-3: Three-Pin Jumper Block Settings

Jumper	Description	* Pins 1-2	Pins 2-3	OFF
K1	CompactPCI/PSB HEALTHY#	Makes the CPC441x drive CompactPCI HEALTHY# TRUE when backend power is good.	Makes the CPC441x drive CompactPCI HEALTHY# TRUE when backend power is good and the switch application is operational.	HEALTHY# is disabled from PCI bus.

* = factory default

When K1 is jumpered 1-2, the **HEALTHY#** signal indicates to a host whether the CPC441x has good power (i.e., whether all four back-end voltages are within tolerance). When K1 is jumpered 2-3, the **HEALTHY#** signal indicates to a host whether the CPC441x has good power and is on-line. The on-line condition implies the following:

- Power-On Confidence (POC) tests have completed successfully
- on-line integrity tests detect no faults
- the watchdog timer is being refreshed

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- no SMB command to enter the fault state has been received

See Chapter 7, “System Management Bus and Intelligent Platform Management,” on page 269 for a description of how to manage the CPC441x fault condition through SMB.

Table 3-4: Four-Pin Jumper Block Settings

Jumper	Description	* Pins 1-2	Pins 2-3	Pins 2-4
K2	CompactPCI Hot Swap	On-board power sequencer enabled by CompactPCI BDSEL	On-board power sequencer always enabled.	On-board power sequencer enabled by SMB controller.

* = factory default

The **BDSEL** jumper (K2) connects the chassis-supplied $\overline{\text{BDSEL\#}}$ signal to the power control circuit, allowing for system-managed power-on of the CPC441x. This jumper must be changed to the 2-3 position if the board is being installed in a PICMG 2.1 High Availability system that does not have a hot-swap controller populated (as is sometimes the case during early system prototyping and development). The default position of 1-2 is used in systems that support the assertion of $\overline{\text{BDSEL\#}}$. This jumper can also be configured (2-4) for $\overline{\text{BDSEL\#}}$ assertion when instructed by the on-board SMB controller.

CPC4411 Port Configuration

A build option provides a CPC4411 PICMG 2.16 Fabric board, supporting up to 24 Link Ports. An alternate build option supports a standalone enterprise switch.

CPC4411F — PICMG 2.16 Fabric Board

The CPC4411F can support up to 19 switched Ethernet ports in a standard fabric application. The switch provides 10/100Mb connectivity to each fabric Link Port. The remaining 10/100Mb ports are supported on the RTM for uplinks. The standard RTM offering is a five port 10/100Mb. The 1000Mb fiber ports are available through the front panel. The CPC4411F populates the J4 connector and cannot be installed into a slot that supports H.110. Ports 20-24 are mapped to J4 in this application.

CPC4411E — Enterprise Board

The CPC4411E can be used as a standalone/enterprise switch. All 24 10/100Mb ports are supported on the RTM in either a dual slot board with 24-ports on RJ45 connectors, or in a single slot using dual RJ21 telco connectors connecting the 24 10/100Mb ports to a patch panel with RJ45 connectors. The fiber ports 25 and 26 are supported out the front panel of the CPC4411E. Since J4 is not populated, the CPC4411E can be used in an H.110 slot, although it is not H.110 capable. It can also be used in a PICMG 2.16 slot, although it is not PICMG 2.16 capable.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

CPC4416 Switch and Jumper Settings

Table 3-5: SW7 Switch Settings

Switch	Description	Open	Closed
1	SMB Enable	Disabled	* Enabled
2	RST_SMB Hard Reset	Disabled	* Enabled
3	SMB_BDSEL	Disabled	* Enabled
4	Reserved	* Disabled	Enabled
5	PCI Reset	* Disabled	Enabled
6	Break Detect	* Disabled	Enabled

* = factory default

When the **SMB Enable** switch is closed, the SMB controller is enabled. When this switch is open, the SMB controller is disabled. The SMB controller will not respond to commands unless it is enabled.

When **RST_SMB** switch is ON (closed), the SMB controller can reset the switch when it receives an IPMI command to do so. See Chapter 7, “System Management Bus and Intelligent Platform Management,” on page 269. When OFF (open), on-board reset is isolated from the SMB controller. Other sources of reset are independent of this setting, such as PCI Reset, Push Button Reset, etc.

When **SMB_BDSEL** is ON (closed) the SMB controller can monitor the PCI bus **BDSEL#** signal. When OFF (open), **BDSEL#** is isolated from SMB. The SMB controller will wait for up to two seconds for BDSEL# to be asserted after power-on before it attempts to acquire the Geographical Address from the backplane and complete its initialization. If **BDSEL#** is not asserted within two seconds, the SMB controller continues its initialization.

The PCI Reset switch connects the on-board reset to the PCI Reset signal. This allows the switch to be reset or not when the CompactPCI bus is reset.

The **Break Detect** switch allows the user to generate a hard reset on the board by sending a BREAK signal in through the console port. This is a useful remote debugging feature.

Table 3-6: SW6 Switch Settings

Switch	Description	Open	Closed
1	User Defined Bit 1 (UDSW1 in MRR)	Set (1)	* Cleared (0)
2	User Defined Bit 2 (UDSW2 in MRR)	Set (1)	* Cleared (0)
3	User Defined Bit 3 (UDSW3 in MRR)	Set (1)	* Cleared (0)
4	User Defined Bit 4 (UDSW4 in MRR)	Set (1)	* Cleared (0)
5	NMI Switch	* Hard Reset	NMI
6	Burn-In Mode (ESS) - Factory Use Only	* Disabled	Enabled

* = factory default

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The status of **User Defined** signals is available via an enterprise MIB variable which is accessible from the CLI and SNMP.

The **NMI** switch selects whether the Watchdog assertion causes a Non-Maskable Software interrupt or a Hard Reset to the switch CPU. If the switch is set to NMI (closed), then the user has the option to allow the switch Operating System to remain running and accessible via the Console and Management Ethernet ports after the watchdog event occurs. This may allow for the diagnosis of the problem that led to the fault. If the NMI switch is set to Hard Reset (open), then a watchdog assertion will reset the switch. If the user enables reboot-on-watchdog (see "Enable or Disable Reboot on Watchdog Timeout" on page 238), then the switch will restart regardless of the NMI switch setting. If the NMI switch is set to NMI (closed), and reboot-on-watchdog is disabled, then the switch will remain offline with the switch Operating System running. If the NMI switch is set to Hard-Reset (open), and reboot-on-watchdog is disabled, then the switch will remain offline in a low-level monitor loop.

Note: *In the case of a Watchdog, the switch Fabric and Node ports are always taken offline and the Fault indicator is illuminated, regardless of the NMI switch setting. If reboot-on-watchdog is enabled, the switch will restart and bring the switch ports back on line, but leave the Fault indicator on.*

The **ESS** function is used only at the factory to burn-in boards and should not be moved by the user.

Table 3-7: Three Pin Jumper Block Settings (K9)

Jumper	Description	Pins 1-2	Pins 2-3
K9	CompactPCI/PSB HEALTHY#	Asserted when PWRG from HSC is true	Asserted when PWRG from HSC is true, the ALIVE bit is set in SCR and no FAULT* condition exists

When K9 is jumpered 1-2, the **HEALTHY#** signal indicates to a host whether the CPC441x has good power (i.e., whether all four back-end voltages are within tolerance). When K9 is jumpered 2-3, the **HEALTHY#** signal indicates to a host whether the CPC441x has good power and is on-line. The on-line condition implies the following:

- Power-On Confidence (POC) tests have completed successfully
- on-line integrity tests detect no faults
- the watchdog timer is being refreshed
- no SMB command to enter the fault state has been received

Table 3-8: Four Pin Jumper Block Settings (K10)

Jumper	Description	* Pins 1-2	Pins 2-3	Pins 2-4
K10	Hot Swap Control	J1-D15 (BDSEL#) to HSC ON# pin	HSC ON# always true	SMB PIC Controller drives HSC ON# pin

* = default

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The **BDSEL** jumper (K10) connects the chassis-supplied $\overline{\text{BDSEL\#}}$ signal to the power control circuit, allowing for system-managed power-on of the CPC441x. This jumper must be changed to the 2-3 position if the board is being installed in a PICMG 2.1 High Availability system that does not have a hot-swap controller populated (as is sometimes the case during early system prototyping and development). The default position of 1-2 is used in systems that support the assertion of $\overline{\text{BDSEL\#}}$. This jumper can also be configured (2-4) for $\overline{\text{BDSEL\#}}$ assertion when instructed by the on-board SMB controller.

If the SMB controller is configured to manage the power sequencer, then the appropriate IPMI command to bring up power on the board must be provided by the BMC (see Chapter 7, “System Management Bus and Intelligent Platform Management,” on page 269). The position of this jumper may need to be changed if the board is installed in a non-hot-swap chassis.

CPC4416 Fabric-to-Fabric Link Port

For PICMG 2.16 fabric slot configurations, the CPC4416 offers a jumper-configurable option to use gigabit port 26 as a fabric-to-fabric link on the CompactPCI/PSB J3 connector, as described in the PICMG 2.16 specification. The alternative is to provide gigabit port 26 to the midplane via J4 to pass through to an RTM which brings it out to a RJ45 connector for external twisted pair connectivity, or provide gigabit port 26 to the PTMC interface.

The CPC4416 fabric slot RTM has a configuration option to use Link Port 24 (100Mb link) to support a fabric-to-fabric link on the CompactPCI/PSB J3 connector as described in the PICMG 2.16 specification. Note that the fabric-to-fabric link will not be supported in an application that uses a PTMC module with no RTM.

CPC4416 Port Configuration

Switches are provided to configure the routing of Link Ports 22, 23 and 25; jumpers are used to configure Link Port 26.

Table 3-9: Port 22 Mapping (SW3)

Port 22 Switches (SW3)	PICMG 2.16 Fabric	PICMG 2.16 Node/Enterprise	PTMC
ON	J4	J5	No
OFF	No	No	Yes (PTMC Port 4)

Table 3-10: Port 23 Mapping (SW4)

Port 23 Switches (SW4)	PICMG 2.16 Fabric	PICMG 2.16 Node/Enterprise	PTMC
ON	J4	J5	No
OFF	No	No	Yes (PTMC Port 3)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 3-11: Port 25 Mapping (SW1, 2)

Port 25 Switches (SW1, SW2)	PICMG 2.16 Fabric	PICMG 2.16 Node/Enterprise	PTMC
ON	J4 (Uplink)	J3 (Node B)	No
OFF	No	No	Yes (PTMC Port 1)

Table 3-12: Port 26 Mapping (K1-8)

Port 26 Jumpers (K1-K8)	PICMG 2.16 Fabric	PICMG 2.16 Node/Enterprise	PTMC
1-2	J3 (F2F)	J3 (Node A)	No
2-3	J4 (Uplink)	No	No
OFF	No	No	Yes (PTMC Port 2)

The CPC4416 has a build option to provide a PICMG 2.16 Fabric board, supporting up to 24 Link Ports. A separate build option supports either a PICMG 2.16 Node board, providing two gigabit Ethernet ports as Link Ports, or a standalone Enterprise switch. Both build options support a PTMC module.

CPC4416F — PICMG 2.16 Fabric Board

The CPC4416F can support up to 19 switched Ethernet ports in a standard fabric application. The PICMG 2.16 Extended Fabric is also supported for the full 24 ports. The CPC4416 provide 10/100Mb connectivity to each fabric Link Port.

The remaining 10/100Mb ports and the two 10/100/1000Mb ports are supported on the RTM for uplinks. The standard RTM offering is a five port 10/100Mb and two 10/100/1000Mb port RTM.

The Fabric-to-Fabric link is supported with the CPC4416F (see “Fabric-to-Fabric (F2F) Link Options” on page 54).

A PTMC module is also supported, for up to four Ethernet ports (see “FlexLink™ Module” on page 505).

The CPC4416F populates the J4 connector and cannot be installed into a slot that supports H.110. Ports 20-26 are mapped to J4 in this application.

CPC4416N — PICMG 2.16 Node Board

The CPC4416N can support dual Link Port applications. The two 10/100/1000Mb switched Ethernet ports are connected to the Node Link Ports. Port 26 is Node Port A. Port 25 is Node Port B.

The 10/100Mb ports are supported on the RTM in either a dual slot board with 24-ports on RJ45 connectors, or in a single slot using dual RJ21 telco connectors connecting to a patch panel with RJ45 connectors.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

A PTMC module is not supported in PICMG 2.16 Node board applications, since the gigabit ports are used for the PICMG 2.16 link ports.

The CPC4416N does not populate the J4 connector, so the board may be used in H.110 systems. Ports 20-24 are remapped with 0-ohm series resistors at the J4 locations to unused J5 pins. Port 8 is also remapped with 0-ohm series resistors to a different location on J3. Port 25 is remapped with 0-ohm series resistors at the J4 location to J3. Port 26 is mapped with jumpers.

CPC4416N — Enterprise Board

The CPC4416N can be used as a standalone/enterprise switch. All 26 ports are supported on the RTM in either a dual slot board with 26 ports on RJ45 connectors, or in a single slot using dual RJ21 telco connectors connecting the 24 10/100Mb ports to a patch panel with RJ45 connectors and two 10/100/1000Mb ports via RJ45s on the RTM. A PTMC module is also supported, for up to four Ethernet ports (see “FlexLink™ Module” on page 505).

Configuring RTMs

Node vs. Fabric Interface

A 24-port double slot RTM (part no. 11639) can be used with either the CPC4411F fabric board (as a standalone switch in a conventional CompactPCI chassis), or the CPC4416N node board (in a PICMG 2.16 chassis). A 4-position microswitch, SW1, allows the user to configure Port 8 to rJ3 as either a node or fabric interface.

- When interfacing to a fabric board (CPC4416F), the switches should be closed (On). This connects Link Port 8 to the RJ45 connector on the RTM.
- When interfacing to a node board (CPC4416N), the switches should be left open (Off). This removes the connection to the RJ45 connector for Link Port 8.

These settings are shown in the following table:

Table 3-13: Port 8 Configuration Switches (SW1)

Bit	Description	Position Description
SW1-1	TX8F+	* ON = for use with CPC4411F as a standalone switch # OFF = for use with CPC4416N as a PICMG 2.16 node board. This configuration disables the port 8 RJ45 connector on the RTM.
SW1-2	TX8F-	
SW1-3	RX8F-	
SW1-4	RX8F+	

* = default when shipped with a CPC4411F

= default when shipped with a CPC4416N

A 26-port double slot RTM (part no. 11640) can be used with either the CPC4416F fabric board or CPC4416N node board to operate as a standalone switch in a conventional CompactPCI chassis. Jumpers K1-K4 allow the user to configure ports 8 and 25 on this RTM as a node or fabric interface:

- When interfacing to a node board (CPC4416N), K1-K4 should be in the 2-3 position (node).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- When interfacing to a fabric board (CPC4416F), K1-K4 should be in the 1-2 position (fabric).

Fabric-to-Fabric (F2F) Link Options

In a PICMG 2.16 chassis with two fabric boards, the user has the option to configure a fabric-to-fabric link. On the CPC4416, the user can choose between a 1000Mb fabric-to-fabric link configurable on the baseboard, or a 100Mb fabric-to-fabric link configurable on the 5-port RTM (part no. 11635).

The SW1 switch on the 5-port RTM is used for configuring the fabric-to-fabric connection in a PICMG 2.16 chassis. Closing all switch sections (i.e., placing them in the ON position) connects Link Port 24 to LPf (A and B) on J3, making possible a fabric-to-fabric connection. These settings are presented in the following table:

Table 3-14: Fabric-to-Fabric SW1 Settings

Bit	Description	Position Description
SW1-1	F2FTX+	ON = Link Port 24 (TX24+) to F2F * OFF = Link Port 24 (TX24+) to RJ45 on rear panel
SW1-2	F2FTX-	ON = Link Port 24 (TX24-) to F2F * OFF = Link Port 24 (TX24-) to RJ45 on rear panel
SW1-3	F2FRX+	ON = Link Port 24 (RX24+) to F2F * OFF = Link Port 24 (RX24+) to RJ45 on rear panel
SW1-4	F2FRX-	ON = Link Port 24 (RX24-) to F2F * OFF = Link Port 24 (RX24-) to RJ45 on rear panel

* = factory default

For diagrams and descriptions of the available RTMs, see Chapter 23, “Rear Transition Modules & Board Pinouts,” on page 491.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Shelf Address

The SW1 microswitch on the 24-port single-slot and the 26-port dual-slot RTMs, and the SW2 microswitch on the 24-port dual-slot RTM, are used to present the Shelf Geographic Address (SGA) in a node slot. The SGA is used by the SMB controller on the CPC441x to form the IPMB Slave Address. When using PICMG 2.9, the user should set this switch to the SGA of the chassis. The switch settings are presented in the following table:

Table 3-15: Shelf Geographic Address Switches (SW1, SW2)

Bit	Description	Position Description
SW-1	SGA4	ON = 0 * OFF = 1
SW-2	SGA3	ON = 0 * OFF = 1
SW-3	SGA2	ON = 0 * OFF = 1
SW-4	SGA1	ON = 0 * OFF = 1
SW-5	SGA0	ON = 0 * OFF = 1
SW-6	Unused	* OFF

* = factory default

Backplane Connector Keys

In accordance with PICMG 2.10 and 2.16, the CPC441x provides backplane connector keys to prevent inadvertent installation in an incompatible backplane slot. The J1/P1 and J4/P4 connectors have provisions for these keys.

The J1/P1 key provides PCI signaling voltage information (3.3 or 5 volt). The CPC441x utilizes a minimal subset of the PCI signals for hot-swap compatibility. These are 5 volt tolerant and will operate at either 3.3 or 5 volts, so no key is installed in J1/P1, indicating universal signaling.

Fabric Board Key (CPC4411F and CPC4416F)

A PICMG 2.16 Fabric Board uses the J4/P4 connector as part of the Ethernet switching fabric, and is thus incompatible with standard telecom backplanes supporting the Computer Telephony Bus (H.110). It is intended for installation in PICMG 2.16 compatible backplanes (fabric slots) only. The J4/P4 key prevents insertion into an incompatible slot. The PICMG 2.16 Standard Fabric Board key:

IEC 61076-4-101 Blue/Lilac (RAL #4005) key (code 2478)

is installed in the connector cavity to provide compatibility with Standard Fabric Board slots (Link Ports 1 through 19 on J3/P3, and J5/P5). Link Ports 20 through 24 are available at the RTM.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Extended Fabric Board Key (CPC4411F and CPC4416F)

The CPC4411F or CPC4416F Fabric Board can be an Extended Fabric Board, meaning that Link Ports 20 through 24 are supported on the J4/P4 connector. The Extended Fabric Board key:

IEC 61076-4-101 Ocher Yellow (RAL #1024) key (code 1235)

is provided in a separate bag for optional installation by customers desiring Extended Fabric Board Slot keying. Pull out the existing key with needle-nose pliers, then snap the new key into place. Make sure your backplane slot has a compatible key.

Node boards do not have the J4/P4 connector installed, and so the key is not applicable.

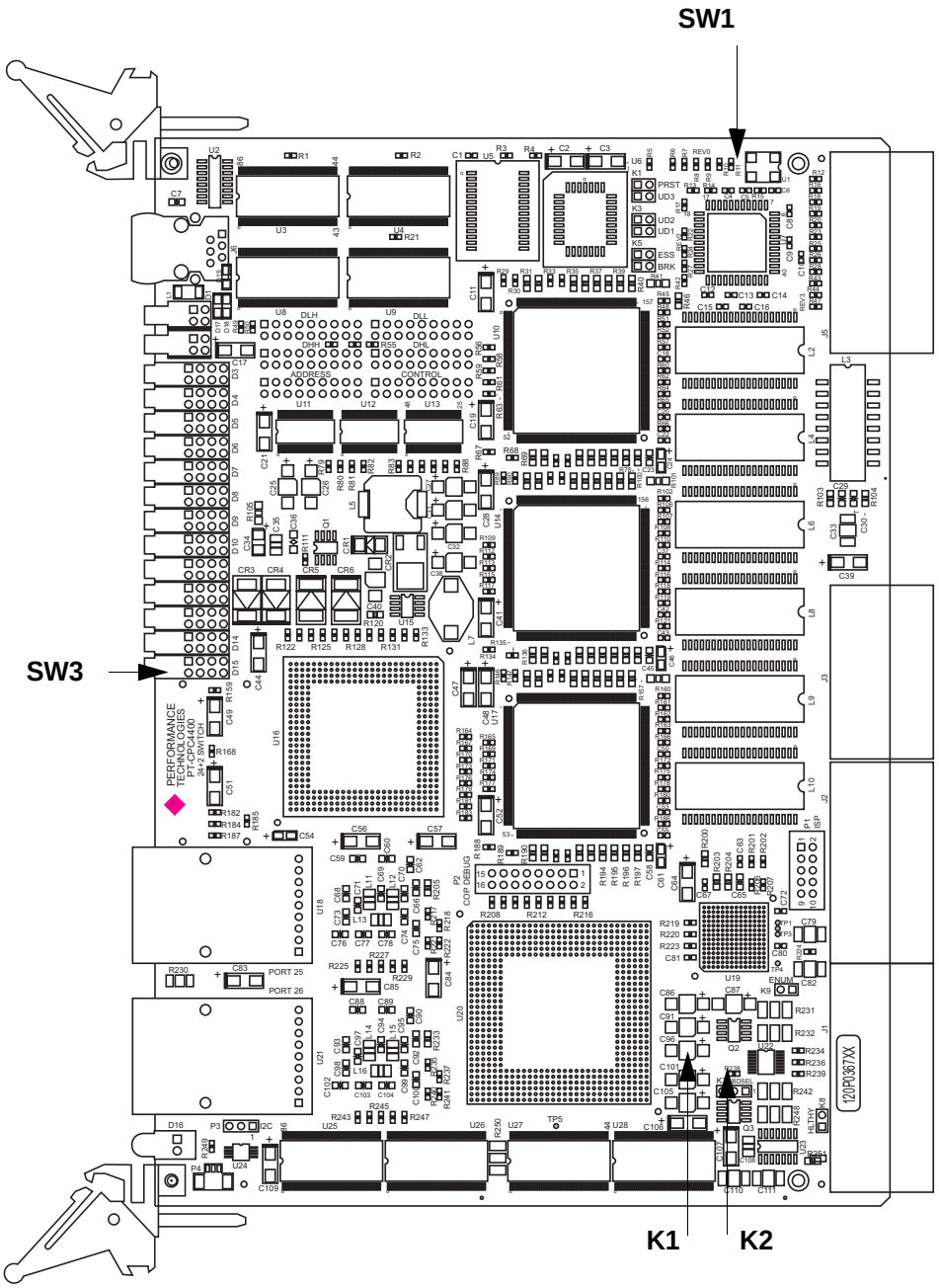
Handle Keys

The CPC441x is shipped with no handle keys installed. A bag of 8 handle keys (Rittal 3684325) is provided with the CPC441x. If it is desired to differentiate slot-specific, user-defined I/O functions, these keys can be installed by the user per PICMG 2.10, “Keying of CompactPCI Boards and Backplanes.”

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

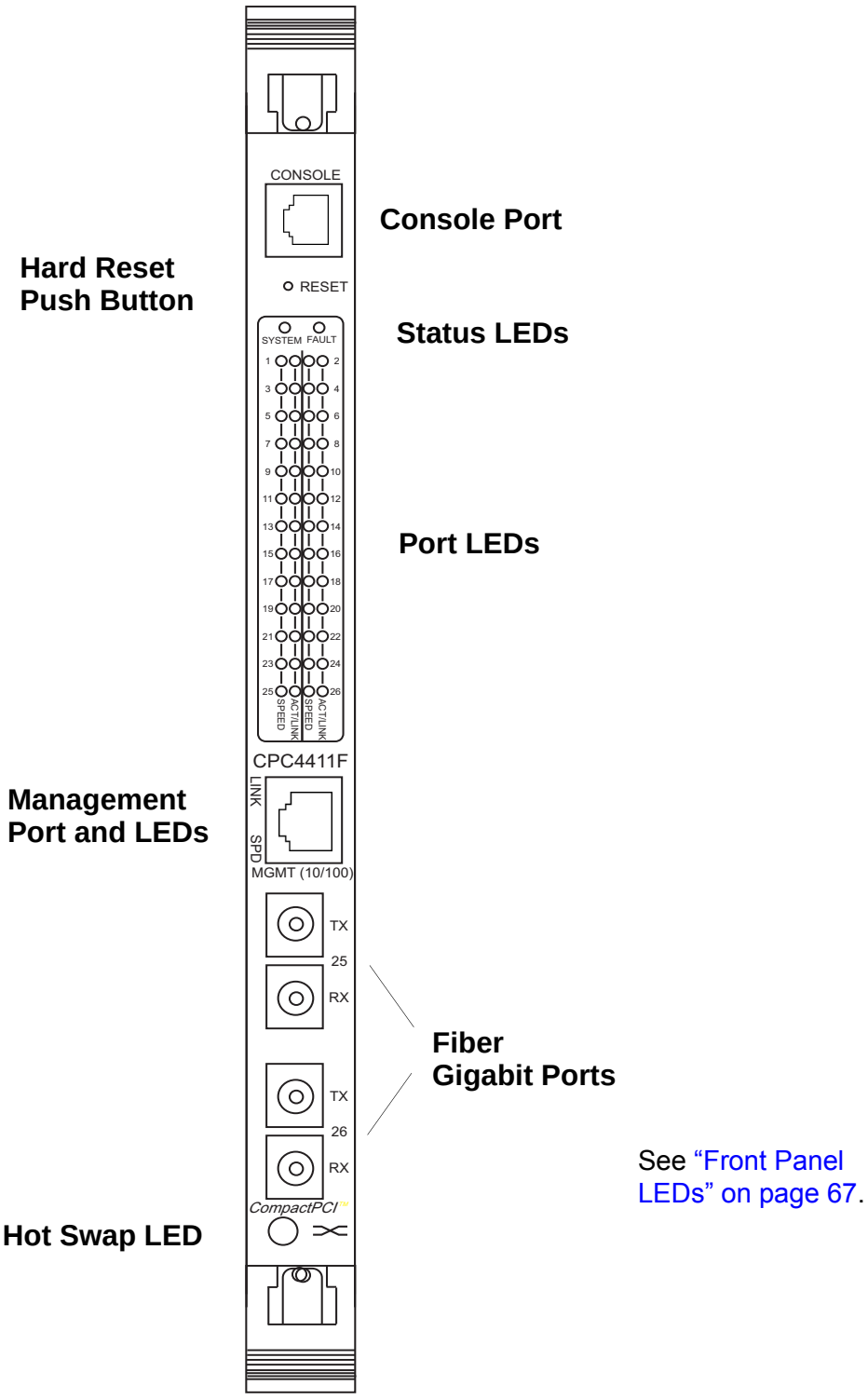
Board Diagrams

Figure 3-1: CPC4411 Board Layout



Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

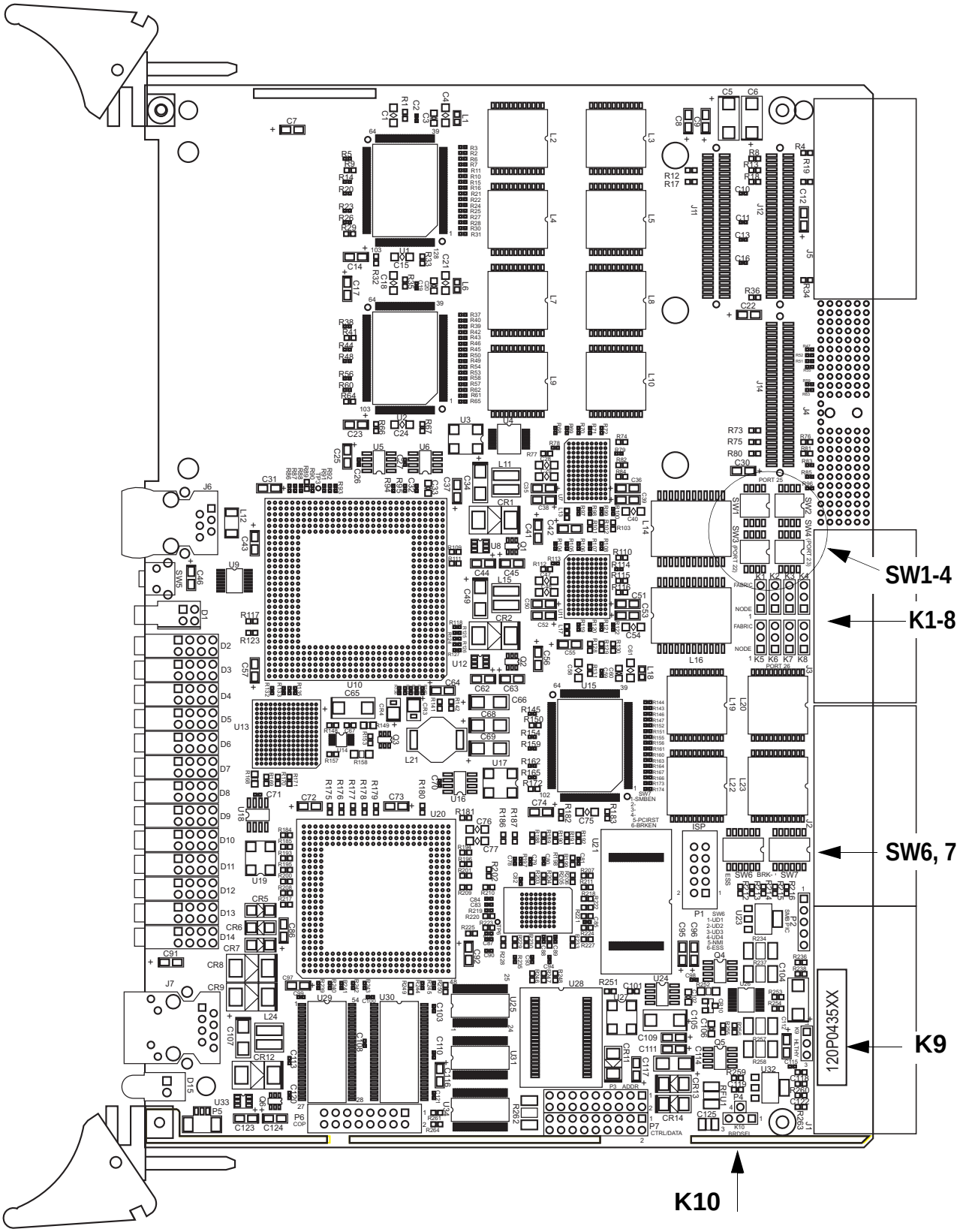
Figure 3-2: CPC4411 Front Panel



See “Front Panel LEDs” on page 67.

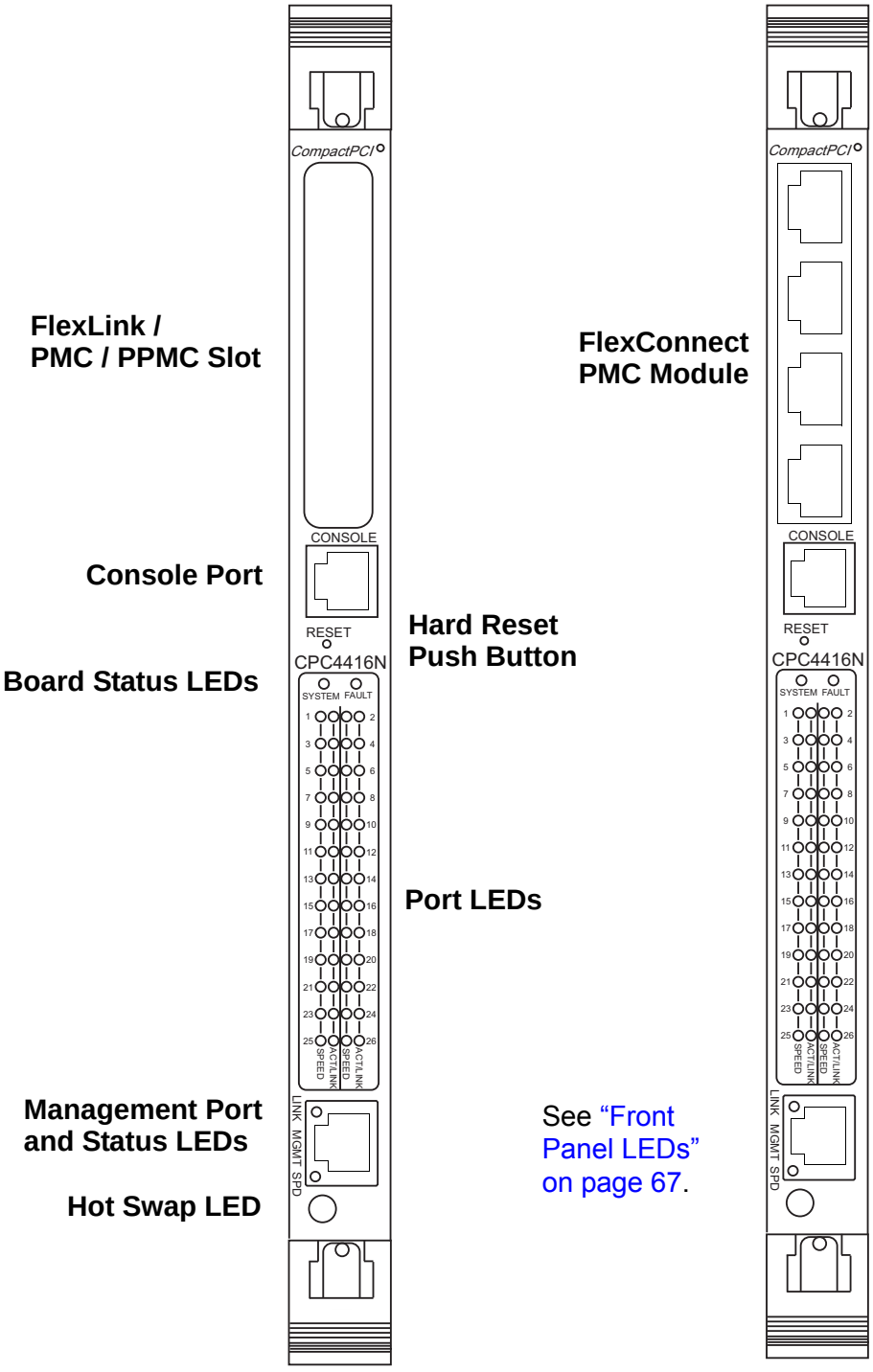
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 3-3: CPC4416N Board Layout



Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 3-4: CPC4416 Front Panels



Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Physical Installation

Before installing the CPC441x, make sure the board is correctly configured for your application. If the board is being installed in a PICMG 2.1 High Availability system that does not have a hot-swap controller (as is sometimes the case during prototyping and development), the BDSEL# jumper will typically have to be changed. In this case, install the “hot-swap” jumper in positions 2-3. See “DIP Switch and Jumper Options” on page 46 for more information.

Installing the CPC441x

The following instructions assume that the chassis power is on and that the host supports hot-swap insertion. If the system does not support hot-swap, power must be turned off prior to installation.

Note: *The CPC441x supports only the hardware connection layer of PICMG 2.1 R1.0 CompactPCI Hot Swap specification (i.e., that portion of “Hot Swap” required by PICMG 2.16 R1.0).*

1. Unlock the ejector handles by depressing the red latch buttons, and then gently slide the CPC441x into the chassis, aligning the board with the guides in the top and bottom of the slot. Press the handles toward each other to lock the board in the chassis.
   When the board makes contact with the CompactPCI backplane, the blue Hot Swap LED turns ON and the hardware connection process begins. When the board is operational, the blue Hot Swap LED turns OFF.
2. Insert the RTM board, if required, into the corresponding I/O slot in the rear of the chassis, and install the port cables to the RTM connectors.

Note: *RTMs may be installed “hot,” but extreme care must be taken to insure proper pin alignment during insertion. RTMs support alignment tabs to aid in insertion.*

3. Reconnect any cables from the peripheral devices.

Removal

To remove the switch

1. Unlock the handles by depressing the red latch button in each handle, and then press the handles away from each other. The board disconnects from the chassis, and the blue Hot Swap LED comes ON.
2. Remove the board from the chassis.

MAC Address Identification

The CPC441x has a unique MAC Address for the following entities:

- each physical port (ap) and its associated aggregator (ag)
- each potential network interface (sw)
- the management Ethernet port (mgmt)

ap*n* are equivalent to physical ports (see Chapter 16, “Link Aggregation,” on page 385). Each is assigned a unique MAC address that is used for Spanning Tree, GVRP, GMRP, and Pause PDUs.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

ag*n* are aggregators (see Chapter 16, “Link Aggregation,” on page 385). IEEE 802.3ad requires a unique MAC address for each aggregator in order to support LACPDUs.

mgmt0 and **sw*n*** are IP subnet interfaces, and each is assigned a unique MAC Address. This MAC Address is used as the Source IP Address in all frames generated by the interface. This address is also provided to hosts using the ARP protocol when the hardware address of the particular interface is requested.

The MAC addresses assigned to these entities on the CPC441x are not sequential when viewed in Ethernet bit order. They are derived from a sequential list of Token-Ring format MAC addresses (this is a result of company history and the manufacturing process). Token Ring format MAC Addresses can be converted to Ethernet addresses by swapping the bit-order within each byte of the address (bit 0 becomes bit 7, bit 1 becomes bit 6, etc.).

Following is the algorithm used to determine the MAC address assignment of an entity:

- mgmt0 is assigned the base address of the board.
- Starting with the next available MAC Address in Token Ring Format, sequentially assign MAC Addresses to the Aggregation Ports (ap0 through ap25) starting with ap0, and to Aggregators (ag0 through ag25) starting with ag0, such that ap*n* MAC Address is the same as ag*n* MAC Address.
- Starting with the next available MAC address in Token Ring Format, sequentially assign MAC Addresses to the sw0 through sw15 interfaces.

The MAC Addresses are also available through the Interfaces MIB (RFC2233). This MIB is accessible through SNMP or locally using the Lua language. A sample Lua script is loaded on the CPC441x that accesses this MIB and dumps the MAC Addresses of each entity to the console. To execute this script, log on to the CPC441x and type:

```
# samples/allmacs
```

Initial Setup

Prior to using the CPC441x in the network, you should establish a compatible configuration. If network management is desired, this includes (at a minimum) setting the IP Address of the Switch Port interface and/or the Out of Band Management Port interface. Since the switch is not yet attached to the network, this initial setup must be done through the console port.

Console Port Connection

Connection to the console port is used for direct local management. The Console port uses RS-232 compatible signal levels, and the terminal (or terminal emulator) connected to the console port must be configured as follows:

- Baud rate — 9600
- Data bits — 8
- Stop bit — 1
- Parity — None
- Flow control — None
- VT-100 Terminal Compatible

The Console port pins are shown in “RS-232 Console Port” on page 498.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Boot Process

The boot process is composed of the following steps:

- Power-On Confidence (POC) Test
- Switch Initialization
- Execute **boot.lua**
- Bring up switch ports
- Initialize TCP/IP
- Execute **rc.lua**

Power-On Confidence (POC) Test

After applying power to the CPC441x, the switch performs a Power-On Confidence (POC) Test. During the POC, all ports are temporarily disabled.

Switch Initialization

After POC is complete, the switch will bring up the switching software tasks and restore its configuration from Flash. The configuration parameters are determined by the contents of the **durable** file located on the CPC441x file system. The **durable** file is processed before running **boot.lua**. All switch ports remain disabled even if the **durable** file indicates that the ports are enabled. This is done to allow **boot.lua** to override link settings that had been saved in the **durable** file.

Note: *On the first boot, there will not be any* ***durable*** *file, so the factory default settings will apply.*

Execute boot.lua

The file **boot.lua** contains a Lua program that may be used to override the non-volatile memory settings stored in the **durable** file prior to enabling any switch ports. Possible uses for this might be to assign IP addresses based on the slot number in which the CPC441x is installed, or to override link settings that had been saved. The Lua scripting language is described in Chapter 21, “Lua Programming Language,” on page 449. All switch ports remain disabled during the execution of **boot.lua**.

Bring Up Switch Ports

After processing **boot.lua**, any switch ports that are enabled will be allowed to establish link.

Initialize TCP/IP Settings

After the switch ports have been allowed to establish link, the TCP/IP stack is initialized. If so enabled, this includes acquiring an IP Address from a DHCP/BootP Server.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Execute rc.lua

The file **rc.lua** contains a Lua program that is run as the final stage of the boot process. Lua is described in Chapter 21, “Lua Programming Language,” on page 449. This program may be modified by the user to customize the CPC441x at boot time for use in a particular application.

Logging In

After the CPC441x has completed the Boot Process, it is operational. Once operational, you can log in to the switch and configure an IP address for each or any of the CPC441x IP interfaces (Out-of-Band Management and up to 16 switch interfaces).

Use the following steps to configure the IP settings of the board:

1. Connect a terminal or workstation running terminal-emulation software to the console port. See “RS-232 Console Port” on page 498 for pin connection information.
2. At the Login prompt, enter admin:

   ```
   Login: admin
   ```

3. At the Password prompt, enter the default Read/Write password (Read/Write access allows you to modify switch settings). For example:

   ```
   Password: password
   ```

4. Assign an IP address and subnetwork mask for each required Switch Port IP Interface. This IP Address may be used to communicate with the CPC441x IP stack via a switch port. A switch interface is always associated with a VLAN. Initially, there is only one VLAN with VLAN ID (VID) of 1. The following example assigns an IP address to that VLAN and creates a switch-based IP Interface. In order to add more switch interfaces, you must first create more VLANs. See “Manage Internet Protocol (IP) Settings” on page 132.

   ```
   # ip config sw0 147.139.1.33 255.255.255.0 1
   ```

5. Assign an IP address and subnetwork mask for the Management Port IP Interface. This IP Address may be used to communicate with the CPC441x IP stack via the Management port only. Be sure that the Management Port IP address is in a different subnet than the Switch Port IP address. For example:

   ```
   # ip config mgmt0 147.139.2.33 255.255.255.0
   ```

   Note: *One less argument is required when setting the management IP address, versus setting a switch interface IP address (VLAN ID is not needed when setting the management IP address).*

6. Make any other changes to the default configuration necessary. For more information, see Chapter 5, “CLI Commands,” on page 73.
7. Save your configuration changes so that they will be in effect after the next switch reboot:

   ```
   # save
   ```

8. When you are finished initializing the configuration, log out of the switch by typing

   ```
   # exit
   ```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The switch can have the IP address set by a BootP or DHCP function as well. See “Manage BootP Settings” on page 82, or “DHCP Client/Server Configuration” on page 91 for more information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

4

Management

Overview

This chapter contains information regarding the front panel LEDs, the Command Line Interface (CLI), SNMP, the HTTP server user interfaces, and security management. The key topics in this chapter include:

- “Front Panel LEDs” on page 67
- “Command Line Interface (CLI)” on page 69
- “Simple Network Management Protocol (SNMP) Agent” on page 70
- “HTTP (Web) Server” on page 70
- “Switch Security” on page 70

Front Panel LEDs

The front panel LEDs are:

- Port LEDs
- Board-level System Status LEDs
- Hot Swap LED

See the front panel diagrams in Figure 3-2: “CPC4411 Front Panel” on page 58 for LED locations.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Port LEDs

The status of the switched Ethernet ports and the out-of-band management port is indicated by LEDs visible from the front panel. A green LED is used to indicate link and activity (transmit or receive) (see Table 4-1), and a yellow LED is used to indicate the current port speed (see Table 4-2).

Table 4-1: Port Link/Activity LED

LED State	Indicates
Green	Link
Blinking Green	Activity (transmit or receive)*
OFF	No Link

* Receive activity for CPC4411 Fiber gigabit (Fx) ports only.

Table 4-2: Port Speed LED

	Indicates			
LED State	Mgmt Port	10/100Mb	10/100/1000Mb Tx	1000Mb Fx
Yellow	100Mb	100Mb	1000Mb	Not Used (always on)
OFF	10Mb	10Mb	10Mb or 100Mb	Not Used

Board-level System Status LEDs

Two LEDs provide board-level system status information.

- A bi-color (green-yellow) LED provides *system* status on the front panel.
- A red LED provides *fault* status on the front panel.

System LED

On power-up, the system LED is yellow. After the basic board integrity checks are complete the system LED changes to green.

The System LED normally remains green unless a board failure is detected. The board failure turns the system LED OFF. See Table 4-4.

Table 4-4: System LED

LED State	Indicates
Green	Board is operational
Yellow	Board is booting
OFF	Fault or no power

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Fault LED

The Fault LED is OFF unless a serious internal error is detected. If a serious error is detected, the red Fault LED turns ON. If the Fault LED is illuminated, the CPC441x will also de-assert the HEALTHY# signal on the CompactPCI bus. To turn off the Fault LED, the CPC441x must be power-cycled or reset via the front panel push button. See Table 4-5. Also see “Fault State” on page 448 for additional information about diagnosing the Fault State.

Table 4-5: Fault LED

LED State	Indicates
Red	Fault
OFF	No fault or no power

Hot Swap LED

During insertion, the blue Hot Swap LED turns ON when the board makes contact with the backplane, and remains on until the board has successfully booted up. It may take 60 seconds or longer for the board to establish itself in the system and turn the blue LED OFF. During removal, the user partially opens the lower ejector handle, which signals to the board that extraction is underway. The user must then wait for the blue Hot Swap LED to turn ON before continuing to remove the board from the chassis. The blue Hot Swap LED indicates that it is safe to remove the board from the chassis. See “Physical Installation” on page 61 for board insertion and removal instructions.

Command Line Interface (CLI)

The CPC441x CLI is available through either the RS-232 Serial Port or via any Ethernet interface using Telnet. The CLI is password protected. Be sure to logout after using the CLI to avoid inappropriate access to the switch. See “Entering Commands” on page 75 for details.

Terminal Types

The CLI makes minimal default assumptions about the user’s terminal: carriage returns don’t imply line feeds; the screen has 24 lines; the backspace character non-destructively moves the cursor to the left (stopping at the left margin); the terminal rings a bell with character code 0x07.

High Level Commands

See Chapter 5, “CLI Commands,” on page 73 for a full description of the available CLI commands.

File Editor

The CLI provides access to a simple line-oriented file editor. This can be used to edit scripts stored in the Flash file system.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Online Help

The CLI provides context sensitive command syntax help. See “Entering Commands” on page 75 for available commands and syntax.

Simple Network Management Protocol (SNMP) Agent

The CPC441x SNMP agent is an SNMP v1/v2C/v3 implementation. The agent responds to a defined set of SNMP client requests and generates the appropriate SNMP traps to respond to CPC441x events.

The Performance Technologies Enterprise MIBs are used for CPC441x-specific parameters that are not supported by the standard MIBs.

The ASN.1 documents that identify the private MIB include: cpc4400.mib, ptiIPMIFRU.mib, and ptiIPMIPM.mib. These ASN.1 files are provided on the CD shipped with the product, and are also stored on the file system of the board. See Chapter 6, “Simple Network Management Protocol,” on page 261.

HTTP (Web) Server

The CPC441x provides an onboard HTTP Server that offers a management interface through a standard web browser. Point your web browser to the IP address of the CPC441x and the CPC441x serves HTTP pages to provide status and configuration management. See Chapter 8, “Web Management,” on page 297.

Switch Security

The switch has a main login and password that are required when accessing the switch via the management port, a Telnet session, or the switch Web pages. The default main login username is ‘admin’ and the default password is ‘password’. To change the username, use the CLI ‘username’ command (“User Login Name Management” on page 249. To change the password, use the CLI ‘password’ command (“Password Management” on page 180).

The switch also has eight possible SNMP community access passwords. By default, only one is enabled for read/write permissions as ‘public.’ The Switch administrator can change these passwords with the CLI command ‘snmp community set’ (“Set the SNMP Community Name and Permissions” on page 218).

In order to improve the security of the switch, the administrator may elect to prevent access to the switch management through the network. The following forms of access control are provided:

- enable/disable Telnet
- enable/disable SNMPv1/v2c PDU processing
- enable/disable SNMPv3 PDU processing
- filtering of packets from hosts specified on an allowed/denied host list.

The access control parameters are initially available through SNMP using the following private Performance Technologies MIB objects from the MIB Group ‘cpc4400SecurityGroup’:

- ‘cpc4400CommonTelnetOnOff’ manages Telnet access

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- ‘cpc4400CommonSNMPV1V2cOnOff’ manages SNMP V1/V2c access
- ‘cpc4400SNMPV3OnOff’ manages SNMP V3 access
- ‘cpc4400CommonSecureHostTable’ manages allowed/disallowed Hosts

The allowed/disallowed host table provides control over which hosts are allowed to manage the switch. The user may specify a subnet mask to allow management from a range of IP Addresses. Access control may also include specific TCP/UDP Port numbers and/or ingress interface. CLI commands are also provided to manage these settings (see “Switch Security” on page 241.)

SSH/SFTP

The switch supports secure remote management and file transfer through SSH and SFTP. SSH is a software based mechanism that automatically encrypts and decrypts messages sent between the client and the server (switch). A client that runs SSH may connect to the switch and manage it via a CLI session without the risk of the traffic being monitored or intercepted. In addition to operating a secure CLI session, the switch supports secure file transfer using SFTP. SFTP operates like FTP except that all network traffic is encrypted and decrypted as with SSH. The switch uses SSHv2 and operates as a server only.

SSH and SFTP are disabled by default. Both may be enabled by using the “sshd enable on” command.

The switch supports both password and public-key authentication for SSH and SFTP. The switch and the SSH client both have a public key that may be exchanged prior to establishing a connection. If these keys are exchanged and installed at each end prior to making a connection, then the switch and the client will use these keys to authenticate each other and allow the session to be established without the need for typing in a password. If the client does not have the switch’s public key or vice-versa, then automatic authentication will fail and the switch will force a password to be provided. This is the same password that is established as the CLI password for Telnet or console-based CLI access. If the proper password is provided, then the session is established.

When the user attempts to connect to the switch, the switch will send its public key to the client machine. If the client does not have the correct key for the switch, then the client will typically display a message that asks the user to verify that the switch is actually the host that the user believes he/she is connecting to. This message typically includes a short (16-digit) fingerprint of the switch’s public key. The switch provides a CLI command that allows the fingerprint of the key file to be displayed (“sshd key export”). This fingerprint should be used to validate that the user has connected to the proper switch. If the user accepts the fingerprint as identifying the switch, the client software typically allows the server’s key to be added to a known_hosts file to avoid this step after the initial connection is established.

In order to prepare for public-key authentication, the user should export the switch’s public key to an ASCII formatted file and then incorporate the contents of this file into the client’s known_hosts file. This process is specific to each client and you should consult the documentation for the SSH client software being used. The public key file for each potential client should be placed on the switch in the directory, “flash:/private” and then each of the client keys needs to be registered in the authorized client key registry. This is done by executing the command, “sshd key add” for each client key. Once client keys have been registered, they may be managed using the “sshd key show” and “sshd key remove” commands.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

SFTP is enabled whenever SSH is enabled. The same authorized access as described for SSH above, applies to SFTP. The password used for SFTP access is the same password as is used for SSH, Telnet and Console access to the CLI.

The steps in a typical SSH login are:

1. Client contacts the server (the CPC441x)
2. Client and server negotiate cipher specified
3. Server identifies itself to the client and provides session parameters
4. Client sends server a session key
5. Both sides turn on encryption
6. Server requires login
7. Secure connection is established.

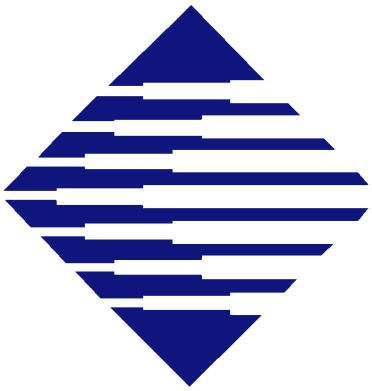
We currently support Diffie-Hellman DSA 512-1024 asymmetric cipher and the following symmetric ciphers:

- AES256-CBC
  RIJNDAEL256-CBC
- AES192-CBC
  RIJNDAEL192-CBC
- AES128-CBC
  RIJNDAEL128-CBC
- 3DES-192-CBC
  ARCFOUR-128

We support the following message authentication codes (MAC):

- HMAC-SHA1
  HMAC-MD5

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Chapter

5

CLI Commands

Overview

This chapter describes the CPC441x CLI (Command Line Interface) commands.

The CPC441x CLI is available on a terminal connected to the front panel or RTM board console port or through a Telnet session from an Ethernet port. The CLI implementation requires a username and password to login. The default username is `admin`, and the default password is `password` (to change the username, see “User Login Name Management” on page 249; to change the password, see “Password Management” on page 180).

The key topics in this chapter include:

- “Conventions” on page 73
- “Entering Commands” on page 75
- “Command Group Summary” on page 78

Conventions

The following conventions are followed in this section:

< > encloses required arguments.

[ ] encloses optional arguments. If < > is found within [ ], then it denotes a required component only when the optional parameter is specified.

| indicates a mutually exclusive choice of options.

{ } encloses a sequence of arguments of the same type.

... indicates that a sequence may continue.

The following data types are used in the command descriptions:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Interface Description

Interface Description specifies an interface using keywords listed in Table 5-1: “Keywords for Interface Types”.

Table 5-1: Keywords for Interface Types

Keyword	Definition
mgmt0	A network interface associated with the management (out-of-band) Ethernet port
sw0-sw15	A network interface associated with the switched (in-band) Ethernet ports

The keyword `mgmt0` specifies the dedicated CPC441x management (out-of-band) Ethernet port. The keywords `sw0-sw15` specify the CPC441x interfaces available to the switched (in-band) Ethernet ports.

List

List is a list of items separated by commas (,) or a range of items specified using a dash (–) (example: 1–12,15,17). No spaces are allowed within the list.

Port

Port is a numeric identifier of a physical Ethernet port. The port numbers are in the range of 1 to 24.

MAC Address

MAC Address is a 6 hex byte, colon-separated description of a MAC Address. Example: 00:c0:8c:00:00:00.

IP Address

IP Address is a 4 decimal byte, dot-separated description of an IP Address. Example: 147.139.1.1.

Boolean

Boolean variables are bi-state, representing true and false. The Boolean keywords shown in Table 5-2: “Boolean Keywords” on page 75 can be used on the command line.

ASCII Label

ASCII Label is a sequence of ASCII characters. It is not quoted and cannot contain spaces.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

ASCII String

ASCII String is a quoted sequence of ASCII characters. Spaces are allowed.

Table 5-2: Boolean Keywords

	ON	OFF
Keywords	on	off
	enable	disable
	true	false
	yes	no

Entering Commands

Commands are organized into hierarchical groups. For example, the command:

```
# snmp target address set <name> [ip] [port] <timeout> <retry> <taglist>
<parameters> <storage>
```

is composed of the major group `snmp`; a subordinate group `target`; the next subordinate group `address`; the command `set`; and the arguments `name`, `ip`, `port`, `timeout`, `retry`, `taglist`, `parameters`, `storage`. The command is always the last word before the arguments.

The actual typed command, with values replacing the argument names, might look like this:

```
# snmp target address set “nms v6” 192.168.1.1 162 1500 3 tmscom “v6
params” nonvolatile
```

The CLI supports the ability to move up and down the command hierarchy narrowing the command set to only those commands below the current context. The user can traverse the command hierarchy by entering the name of a group. The prompt position (defaults to **#**) indicates where on the hierarchy level the command currently exists. Only commands at or below the current context are available to the user. Enter a carriage return by itself on a line to move up one level in the command hierarchy. For example, the `snmp target address set` command entered above could also be entered with this sequence (bold type indicates typed commands):

```
# snmp
snmp# target
snmp target# address
```

Type a question mark (?) to display online Help for each command:

```
snmp target address# set ?
```

Type `help` or a question mark at any prompt to see what commands are available at that level.

In commands with multiple optional arguments, the argument name becomes a keyword. In the following command, `tagged`, `untagged`, and `forbidden` are optional arguments:

```
vlan create  <vid> <vlan_name> [tagged] [untagged] [forbidden]
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The argument `untagged` can be individually specified by typing the argument name, followed by an equal sign and then a value. Use no spaces between the keyword, equal sign, and value.

To specify just the untagged ports, type the following:

```
vlan create <vid> <vlan_name> untagged=1–12,15,17
```

Command Line Editing

Several keystroke commands are available to make command line editing easier.

Table 5-3: Control-Key Commands for Line Editing

Key Combination	Function
Control A	Move to the beginning of the line.
Control B	Move left (backwards) one character
Control D	Delete character
Control E	Move to end of line
Control F	Move right (forward) one character
Control H	Delete one character before cursor (backspace key)
Control I	Complete filename (tab key)
Control J	Done with line (return key)
Control K	Delete to end of line (or column)
Control L	Redisplay line
Control M	Done with line (alternate return key)
Control N	Get next line from history list
Control P	Get previous line from history list
Control R	Search backward through the history list for a particular string.
Control T	Transpose characters
Control V	Insert next character, even if it is an edit command
Control W	Wipe to the mark
Control XX	Exchange current location and mark
Control Y	Retrieve last deleted text
Control [	Start an escape sequence (escape key)
Control]	Move forward to next character “c”
Control ?	Delete character before cursor (delete key) [n]

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 5-4: Esc-Key Commands for Line Editing

Key Combination	Function
ESC Control H	Delete previous word (backspace key)
ESC DEL	Delete previous word (delete key)
ESC SP	Set the mark (space key); see ^X^X and ^Y above
ESC .	Get the last (or [n]'th) word from previous line
ESC ?	Show possible completions
ESC <	Move to start of history list
ESC >	Move to end of history list
ESC b	Move backward a word
ESC d	Delete word under cursor
ESC f	Move forward a word
ESC l	Make word lowercase
ESC m	Toggle if 8-bit chars display normally or with ``M-'' prefix
ESC u	Make word uppercase
ESC y	Retrieve last deleted text
ESC w	Select text
ESC nn	Set repeat count to the number

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Command Group Summary

Specific commands are described under the group headings shown in Table 5-5:

Table 5-5: CLI Command Group Summary

Command Function	See details
Beacon Configuration	Page 79
BootP Settings	Page 82
Class of Service (COS)	Page 85
Console Port Settings	Page 88
Date and Time	Page 90
DHCP Client/Server Config	Page 91
Event Manager	Page 96
File System Management	Page 100
File Transfer	Page 106
Filter Mask Commands	Page 110
Filtering Database	Page 115
GARP Management	Page 120
GMRP and Multicast Policy	Page 122
GVRP Management	Page 125
Command History	Page 128
IGMP Snooping	Page 129
IP Management	Page 132
IPMI:FRU	Page 138

Command Function	See details
IPMI: PM Controller	Page 149
Link Aggregation	Page 152
Log Management	Page 172
Network Diagnostics	Page 175
Online Integrity Tests	Page 178
Password Management	Page 180
Port Commands	Page 181
Routing Management	Page 186
Shell Commands	Page 208
SNMP Configuration	Page 211
Spanning Tree Management	Page 225
Switch Management	Page 237
Switch Security	Page 241
Thresholds	Page 247
User Login Name Management	Page 249
VLAN Commands	Page 250
VRRP Management	Page 254

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Beacon Configuration

The beacon command invokes a signal that informs a host that the switch is running, and that it has network connectivity. Beacon messages are not a guarantee of correct switch and/or network operation, but they can indicate proper functioning. Likewise, an absence of beacon messages can be taken as an indication of a failure.

The switch will send beacon messages using a specified interface to a destination address/UDP port at the specified interval. Using an IP multicast address as the destination (e.g. 224.1.2.3) allows all interested hosts to receive the beacon messages while not placing a burden on other hosts. For those hosts unable to process IP multicast packets, individual beacons can be created.

A beacon instance is associated with a destination IP address (usually a multicast), a destination UDP port number, and a source IP address. These three values uniquely identify a beacon instance. To send beacon messages on multiple subnets, create a beacon for each subnet, using the IP address of the interface as the source IP address.

Beacon packets take the following format:

2 bytes - beacon packet format version (currently 1)

2 bytes - total packet length, 8 header bytes + n user bytes

4 bytes - current time stamp in network byte order.

n bytes - the user data

Note: *The time stamp is standard UNIX time (number of seconds since 1/1/1970 00:00:00). It is in network byte order, which means on the receiving end, if you are writing an application in a POSIX environment, you would use the function ntohl() to get the data back into a host specific byte order.*

Create a Beacon

Synopsis

`beacon create <dst_addr> <dst_port> <src_addr> [time_delay] [ttl] [priority] [user_data]`

where

`dst_addr`	is the IP address to which beacon messages will be sent.
`dst_port`	is the UDP port number to which beacon messages will be sent.
`src_addr`	is the local IP address from which beacon messages will be sent. Set this to 0.0.0.0 if INADDR_ANY is to be used.
`time_delay`	is the time interval between messages, in tenths of a second. The default is 10 (one second).
`priority`	is a value between 5 and 255 used to prioritize the beacon with other switch functions. The default is 48.
`ttl`	is the IP address to which beacon messages will be sent.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

user_data is the data to be included in the beacon message. Maximum size is 255 bytes.

Description

Create a beacon entry.

Destroy a Beacon

Synopsis

beacon destroy <dst_addr> <dst_port> <src_addr>

where

dst_addr is a destination IP address.

dst_port is a destination UDP port.

src_addr is a source IP address of an interface on the switch. Set this to 0.0.0.0 if INADDR_ANY is to be used.

Description

Destroy a beacon entry.

Display a Beacon

Synopsis

beacon display

Description

Display all beacon entries.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Beacon Configuration Examples

The following commands will create vlan 2 and configure network interface sw0 on vlan1 and sw1 on vlan2:

```
vlan remove 1 untagged=4-8
vlan create 2 vlan2 untagged=4-8
ip config sw0 10.1.1.1 255.255.255.0 1
ip config sw1 10.2.2.2 255.255.255.0 2
```

The following command will create a beacon on sw0 at a frequency of twice a second:

```
beacon create 224.1.2.3 5678 10.1.1.1 5
```

The following command will create a beacon on sw1 at the default frequency of once a second:

```
beacon create 224.1.2.3 5678 10.2.2.2
```

The following command will create a beacon to a specific host on sw1:

```
beacon create 10.2.2.10 5678 10.2.2.2
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Manage BootP Settings

Enable or Disable BootP

Synopsis

`bootp enable <interface> [enable]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable BootP on the CPC441x. If no argument is provided, display the current configuration.

Display or Set BootP VLAN ID (VID)

Synopsis

`bootp vid <interface> [vid]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`vid` is decimal integer between 1 and 4094.

Description

Specify the VLAN for which the BootP client should send out its request. You must use a valid VID. If no argument is provided, display the current configuration.

Display or Set BootP Client Interface Name

Synopsis

`bootp ifname [interface]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

Description

Set the interface for which the BootP client is to send out its request. If no argument is provided, display the current value.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set the BootP Timeout Value

Synopsis

`bootp timer <interface> [timeout]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`timeout` is a decimal integer representing seconds.

Description

Set the timeout period to wait for a BootP reply at initialization, if BootP is enabled. “0” (zero) indicates no time limit.

Note: *The CPC441x will not complete the boot process and provide access until either it is issued a lease or BootP times out.*

Configure BootP Client

Synopsis

`bootp add <interface> <vid> [timeout]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`vid` is decimal integer between 1 and 4094.

`timeout` is a decimal integer representing the number of seconds.

Description

Enable a BootP client listening on a particular interface to acquire its IP address at initialization. A VID must exist and be assigned as unique to this interface as well. All sw interfaces are valid. Timeout is the time in seconds before the BootP client fetch of an IP address gives up trying.

Remove BootP Client

Synopsis

`bootp remove <interface>`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

Description

Remove the BootP entry identified by the interface. All sw interfaces are valid.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display All Configured BootP Clients

Synopsis

```
bootp show
```

Description

Display the configured BootP information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Manage Class of Service (COS) Settings

Enable or Disable COS Processing

Synopsis

`cos port enable [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the CPC441x from using Class of Service. When COS is disabled, all traffic is given the same priority. If no argument is provided, display the current configuration.

Display or Set the Default COS for a Port

Synopsis

`cos port priority <portlist> [priority]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`priority` is a decimal integer in the range 0 to 7.

Description

Set the default priority to assign to frames received on the ports defined by `portlist`. Untagged frames will be assigned this priority at the specified ingress port(s). If no argument is provided, display the current configuration.

Packets that are tagged are prioritized based on the priority field in the tag. If the packet is not tagged, the prioritization will be determined by the port priority.

Display the Current COS Queue Configuration

Synopsis

`cos queuing show`

Description

Displays the queuing algorithm, the queue priority mapping, the bounded delay value if bounded delay algorithm is ON, and the queue weighting if weighted or bounded delay is ON.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set the Mapping for Priority to Queue

Synopsis

`cos queuing map <priority> <queue>`

where

`priority` is a integer value between 0 and 7 specifying the tagged frame priority.

`queue` is a integer value between 0 and 3 indicating the queue-priority in the board. Queue 3 is the highest priority queue and 0 is the lowest priority.

Description

Frames either arrive tagged, or are tagged at the ingress port with a particular priority value. (See “Display or Set the Default COS for a Port” on page 85.) The frame is then placed on the queue which corresponds to the tagged-priority value.

This command is used to map a tagged-frame priority value (0–7) to one of the 4 available COS queues. The four queues (0–3) provide 4 levels of frame-priority in the switch.

There is complete flexibility when mapping the tagged-frame priority to the queues. For example, a tagged-frame priority of 7 can be mapped to a queue priority of 3, 2, 1 *or* 0.

Set the COS Queuing Algorithm to Weighted Round Robin

Synopsis

`cos queuing algorithm weighted <w0> <w1> <w2> <w3>`

where

`w0–w3` are used to indicate the number of weighted frames in the queue. Allowed values are integers between 0 and 255. w3 must be greater than or equal to w2, which must be greater than or equal to w1, which must be greater than or equal to w0.

Description

This transmission algorithm services each queue (0–3) in a round-robin fashion. The weight of each queue is specified in number of frames. The algorithm services no more than the number of frames, specified in weight, on each queue before moving to the next queue in a round-robin fashion.

Set the COS Queuing Algorithm to Strict

Synopsis

`cos queuing algorithm strict`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Strict priority is given to servicing the frames on the highest priority queue first, then the frames of the lower queues are serviced in their priority order.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Console Port Settings

Set Console Port Baud Rate

Synopsis

`console baud [rate]`

where

`rate` is a baud rate selection. The allowed baud rate values are:

- 2400
- 9600
- 19200
- 38400

Description

Set or view the console serial port bit rate. If no argument is provided, the current baud rate setting is displayed.

Set Console Display Height

Synopsis

`console lines [count]`

where

`count` is the number of lines in the console display. Allowable values are positive integers greater than one.

Description

Set or view the terminal vertical size in lines of text when connected to the console port. If no argument is provided, the current text line setting is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Console Display Width

Synopsis

`console columns [count]`

where

`count` is the number of characters displayed in one line on the terminal display. Allowable values are positive integers greater than one.

Description

Set or view the terminal horizontal size in characters of text when connected to the console port. If no argument is provided, the current text column setting is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Date and Time

Display or Date and Time

Synopsis

`date [HH:MM:SS[mm/dd/yyyy] ]`

where

mm	is an integer value between 1 and 12 for month.
dd	is an integer value between 1 and 31 for the day.
yyyy	is an integer value for the year.
HH	is an integer value between 00 and 24 (military time) for the hour.
MM	is an integer value between 0 and 59 for the minute.
SS	is an integer value between 0 and 59 for seconds.

Description

Set the current date and time. If no arguments are provided, display the current setting.

Set the Time from a Remote NTP Server

Synopsis

`gettime <ip_addr> [service]`

where

ip_addr	is an IP Address (see “IP Address” on page 74.)
service	is a keyword, either `ntp` or `time`.

Description

Set the system clock from either a remote NTP (Network Time Protocol) server using the NTP protocol, or from a time server running the Time protocol (port 37). The default is NTP. The board clock will be set to Universal Coordinated Time (UTC). The time server may be set up on the local network, or it may be accessed from an internet-based time server over the network.

Additional information regarding the time standard is available at: http://www.time.gov/

A list of NIST (National Institute of Standards and Technology) Network Time servers is available at: http://www.boulder.nist.gov/timefreq/service/time-servers.html

The following IP addresses are assigned to U.S. government NTP time servers: 192.43.244.18 (time.nist.gov), 192.5.41.40 (tick.usno.navy.mil), 192.5.41.41 (tock.usno.navy.mil)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

DHCP Client/Server Configuration

Enable or Disable DHCP Client

Synopsis

`dhcp client enable <interface> [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

`interface` is an Interface Description keyword (See “Interface Description” on page 74.) The valid keywords for this argument are `sw`*n* and `mgmt0`. `sw`*n* indicates one of the switch IP interfaces; only one sw interface supports DHCP at a time. `mgmt0` indicates the out-of-band Ethernet management port.

Description

Enable or disable the DHCP client listening on a particular interface to acquire its IP address at initialization. If no argument is provided, display the current configuration.

Note: *When using the client, if there is no response from any server, the boot time will increase by approximately 90 seconds.*

Set DHCP Client Listen Port

Synopsis

`dhcp client listenport <interface> [port]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`port` is an integer representing a UDP logical port number.

Description

Set the logical port on which the DHCP client listens. If no argument is provided, display the current configuration.

Set DHCP Client Transmit Port

Synopsis

`dhcp client transmitport <interface> [port]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

port is an integer representing a UDP logical port number.

Description

Set the logical port on which the DHCP client transmits. If no argument is provided, display the current configuration.

Display or Set DHCP Client VLAN ID

Synopsis

dhcp client vid <interface> [vid]

where

interface is an Interface Description keyword (See “Interface Description” on page 74.)

vid is decimal integer between 1 and 4094.

Description

Set the VLAN for which the DHCP client should send out its request. Must use a validly configured vid. If no argument is provided, display the current configuration.

Display or Set the DHCP Client ID

Synopsis

dhcp client id <interface> [value]

where

interface is an Interface Description keyword (See “Interface Description” on page 74.)

value is a string of hexadecimal values.

Description

Display or set the DHCP Client ID that is supplied with DHCP Request packets sent by the switch. The string may be up to 255 hex digits. If no value is provided, the current value is displayed.

Display or Set the DHCP Client Retry Count

Synopsis

dhcp client retries <interface> [value]

where

interface is an Interface Description keyword (See “Interface Description” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

value is a decimal number between 0 and 2147483647.

Description

Display or set the DHCP client retry count. The value 0 means try forever. This parameter dictates how many DHCP/BootP requests are made before giving up. If no value is provided, the current value is displayed.

Configure DHCP Client

Synopsis

dhcp client add <interface> <vid> [retries] [trans_port] [rcv_port] [client_id]

where

interface is an Interface Description keyword (See “Interface Description” on page 74.)

vid is decimal integer between 1 and 4094.

retries is a decimal number between 0 and 2147483647. This parameter specifies how many DHCP/BootP requests are made before giving up.

trans_port is an integer representing a UDP logical port number.

rcv_port is an integer representing a UDP logical port number.

client_id is a string of hexadecimal values that is supplied with DHCP Request packets sent by the switch. The string may be up to 255 hex digits.

Description

Enable the DHCP client listening on a particular interface to acquire its IP address at initialization. A unique VID must be assigned to this interface. All sw interfaces are valid.

Remove the DHCP Client

Synopsis

dhcp client remove <interface>

where

interface is an Interface Description keyword (See “Interface Description” on page 74.)

Description

Remove the DHCP entry identified by the interface. All sw interfaces are valid.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display All Configured DHCP Clients

Synopsis

dhcp show

Description

Display the configured DHCP information.

Enable or Disable the DHCP Server/Relay Agent

Synopsis

dhcp server enable [enable]

where

enable is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the DHCP server/relay agent on the CPC441x. If no argument is provided, display the current configuration. The server/relay agent configuration is based on the DHCP configuration file.

Set the DHCP Server Configuration File

Synopsis

dhcp server configfile [conffile]

where

conffile is an ASCII Label up to 40 characters.

Description

Set the DHCP configuration filename to the specified name and path. If no name is provided, display the current name.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set the DHCP Server Logging Level

Synopsis

`dhcp server log [level]`

where

`level` is a keyword consisting of none, error, or all.

Description

Set the current logging state of the DHCP server. If no argument is provided, the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Event Manager

The event names listed in Table 5-6: “Event Names and Descriptions” can be specified in commands that use a specific event name. The quotation marks (single or double) must be included. See the `event` CLI commands that follow Table 5-6:

Table 5-6: Event Names and Descriptions

Event Name	Description
“cold start”	Any instance when the CPC441x boots.
“link down” [1]	A port has lost link. This event “passes” an argument named portNumber which is set to the port number which lost link.
“link up” [1]	A port has detected a new link. This event “passes” an argument named portNumber which is set to the port number which detected link.
“AP link down” [1]	A port has lost link. This event “passes” an argument named portNumber which is set to the port number which lost link (same as “link down” for backwards compatibility).
“AP link up” [1]	A port has detected a new link. This event “passes” an argument named portNumber which is set to the port number which detected link (same as “link up” for backwards compatibility).
“AG link down” [1]	An aggregator port has lost link. This event “passes” an argument named portNumber which is set to the aggregator port number which lost link.
“AG link up” [1]	An aggregator port has detected a new link. This event “passes” an argument named portNumber which is set to the aggregator port number which detected link.
“SW link down” [1]	A switch interface has lost link. This event “passes” an argument named portNumber which is set to the switch interface which lost link.
“SW link up” [1]	A switch interface has detected a new link. This event “passes” an argument named portNumber which is set to the switch interface which detected link.
“auth failure”	A user attempted to access the switch via SNMP with an invalid password or community string.
“1493 new root”	The network Root Bridge has changed.
“1493 topology”	A Spanning Tree topology change has occurred in the network.
“boot save nvm”	The Boot PROM was written. This occurs during installation of new firmware.
“app save nvm”	The Application Flash was written. This occurs during installation of new firmware.
“data save nvm”	The **durable** and **persist** files were modified. This occurs when the user executes the save command. Both files are written when the save command is executed, so the script is invoked twice. The file that changed is passed as an argument named fileName to the script.
“mgmt link down”	The management port has lost link.
“mgmt link up”	The management port has detected link.
“hot swap”	The ejector handle was unlatched.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 5-6: Event Names and Descriptions *(Continued)*

Event Name	Description
“RMON Rising Alarm”	An RMON threshold was crossed where value is increasing.
“RMON Falling Alarm”	An RMON threshold was crossed where value is decreasing.

1. This event may take an optional `portlist` to restrict the events to the specified ports. See “Optional Portlist” below.

Register a Script to Invoke upon Detection of an Event

Synopsis

`event add <event> <script>`

where

`event` is an ASCII String representing the event to be detected. See the event names listed in Table 5-6: “Event Names and Descriptions” on page 96.

`script` is an ASCII Label specifying an existing CLI script filename and path.

Description

Register with the Event Broker to execute the script file, script when the specified event occurs. Each event has a unique set of arguments passed to the provided script. Be sure to provide the full pathname of the script, e.g., `flash:/hotswap.lua`.

Optional Portlist

The following events may take an optional `portlist` to restrict the events to the specified ports, where `portlist` is a List of Port numbers (see “List” and “Port” on page 74):

- "link down"
- "link up"
- "AP link down"
- "AP link up"
- "AG link down"
- "AG link up"
- "SW link down"
- "SW link up"

For example, `event add "link down 6,8,10-12" scriptname.lua` will restrict the link down event to ports 6, 8, 10, 11, and 12.

Multiple events may be added with the same event name and different port lists. In this case, the port lists will be logically ORed. If no port list is given, the command will function with all ports. If the scriptnames are different, the LAST scriptname entered will be used for all ports. Since the port number is passed as an argument to the LUA script, different LUA scripts for different ports should not be required.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

If a portlist is given with an `event remove` CLI command, only those specified ports will be removed, all other ports (if any) will still trigger the event.

Allowable Port Numbers

The "link up" and "link down" events allow port numbers in the range of 1 through 26 on the 4411 and 4416. The "AP link up", "AP link down", "AG link up" and "AG link down" events allow port numbers in the range of 0 through 25 on the 4411 and 4416. The "SW link up" and "SW link down" events allow port numbers in the range of 0 through 15.

Notes:

- *The `event list` CLI command will print the applicable port numbers with the event name. However, this field is limited to 30 characters, so a long portlist MAY be truncated.*
- *Specifying a portlist with other event names will produce the warning message* "Warning - Port list ignored for event <eventname>"*. The command will be accepted.*
- *Specifying an invalid portlist will produce the error message* "Error - Invalid port list <portlist>"*. The command will be rejected.*

De-register a Script When an Event is Detected

Synopsis

`event remove <event>`

where

`event` is an ASCII String representing the event to be detected. See the event names listed in Table 5-6: “Event Names and Descriptions” on page 96.

Description

Remove a previous registration with the Event Broker to execute a script when the specified event occurs.

Optional Portlist

Several events may take an optional `portlist` to restrict the events to the specified ports, where `portlist` is a List of Port numbers (see “List” and “Port” on page 74).

See “Optional Portlist” on page 97 for a description of this functionality as it applies to the `event remove` CLI command.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

List Events Currently Registered through the CLI

Synopsis

`event list [event]`

where

`event` is an ASCII String representing the event to be detected. See the event names listed in Table 5-6: “Event Names and Descriptions” on page 96.

Description

Display the status of the current registration of the named event. Show whether the event has a registration or not, and if so, display the name of the registered script. If no argument is provided, display all existing registrations.

Optional Portlist

Several events may take an optional `portlist` to restrict the events to the specified ports, where `portlist` is a List of Port numbers (see “List” and “Port” on page 74).

See “Optional Portlist” on page 97 for a description of this functionality as it applies to the `event list` CLI command.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

File System Management

For the following Flash file system commands, *filespec* refers to the name of a file. The *filespec* can be an absolute or relative path to the file. Absolute pathnames begin with a forward slash (/), and each forward slash represents a directory level, as in UNIX. The file system name may be provided with an absolute filespec, as in `flash:/temp`.

Note: *filespec is not case sensitive; a file named abc is accessible as ABC, or aBC, etc.*

List the Files in the File System

Synopsis

`list [directory]`

where

directory is an ASCII Label.

Description

List all files located in the specified directory or if no directory is specified, list the contents of the current directory.

Mount a File System

Synopsis

`mount [mountpt] [hostip] [user_name] [password]`

where

mountpt is an ASCII String identifying the name to assign to the local mount point. The mount point must include a colon (:), as in "`root:`".

hostip is an IP Address type specifying the IP address of the file server (see "IP Address" on page 74.)

user_name is an ASCII Label specifying the user ID for the session.

password is an ASCII Label specifying the password for the specified user.

Description

Mounts a remote file system and assigns it a name. If the *user_name* and *password* are entered on the command, they will be displayed in clear text; if the *user_name* and *password* are not entered with the command, the user is prompted to enter the user name and associated password. The entered password will not be displayed. If no arguments are supplied, the current mount points will be displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Remove a Mount Point

Synopsis

umount <mountpt>

where

mountpt is an ASCII String identifying the name to assign to the local mount point. The mount point must include a colon (:), as in "root:".

Description

Removes the specified mount point.

Create a New Level (Directory) within the Directory Hierarchy

Synopsis

mkdir <directory>

where

directory is an ASCII Label.

Description

Create a new directory at the current position.

Note: *A directory cannot be created with the same name as an existing file.*

Check File System for Errors

Synopsis

chkdsk [device]

where

device is an ASCII Label.

Description

Check the device specified by device for errors, and if any errors are found correct them. If no device is specified, flash:/ is assumed.

Note: *chkdsk cannot be used on a mounted file system.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Change Positions Within the Directory Hierarchy

Synopsis

`cd <directory>`

where

`directory` is an ASCII Label.

Description

Changes the current working directory to the specified directory. A colon and slash (:/) are required after specifying a mounted directory.

Example: `cd flash:/temp`

Display the Current Working Directory

Synopsis

`pwd`

Description

Display the absolute path of the current working directory.

Remove a File

Synopsis

`remove <filespec>`

where

`filespec` is an ASCII Label.

Description

Remove the specified file at the current working directory level.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Copy a File

Synopsis

`copy <filespec1> <filespec2>`

where

`filespec1` is an ASCII Label.

`filespec2` is an ASCII Label.

Description

Copies the file specified by *`filespec1`* to the file specified by *`filespec2`*. A new file named *`filespec2`* will be created if one does not already exist.

Rename a File

Synopsis

`rename <filespec1> <filespec2>`

where

`filespec1` is an ASCII Label.

`filespec2` is an ASCII Label.

Description

Changes the name of *`filespec1`* to *`filespec2`*.

Edit a File

Synopsis

`edit <filespec>`

where

`filespec` is an ASCII Label.

Description

Invokes the line editor on the file named, *`filespec`*. The line editor uses the same command set and syntax as the UNIX *ed* command. When in the *ed* editor the command line prompt is a colon (`:`). Use `q <cr>` to return to the CLI.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The following basic commands shown in Table 5-7 are used in the *ed* line editor:

Table 5-7: Basic *ed* Commands

Command	Description
a	Append (create) text after the current line. If you are creating a new file, a puts your text in line 1.
d	Remove current line.
i	Insert (create) text before the current line.
p	Print (display) current line.
q	Quit (end) the line editor session.
.	Stops create mode.
w	Writes the file.

The following URLs contain complete descriptions of command syntax for the *ed* editor:

http://www.cs.ucf.edu/~eke/unixIntro/edSum2.html

http://www.delorie.com/gnu/docs/ed/ed_1.html

Save the Switch Configuration

Synopsis

`save`

Description

The switch configuration (all MIB parameters that are marked ‘durable’) are saved in the file named **durable**.

Compare Files

Synopsis

`cmp <filespec1> <filespec2>`

where

`filespec1` is an ASCII Label.

`filespec2` is an ASCII Label.

Description

Compare the file specified by `filespec1` to the file specified by `filespec2`. If the files are different, the message `files are different` is displayed. If the files are the same, the message, `files match` is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Check for the Existence of a File

Synopsis

`exists <filespec>`

where

`filespec` is an ASCII Label.

Description

If the file specified by `filespec` exists, TRUE is displayed. If the file does not exist, FALSE is displayed.

Display Contents of a File

Synopsis

`more <filename>`

where

`filename` is an ASCII Label.

Description

Display the contents of the file specified by `filename`. The file should contain only printable characters.

Capture Current Configuration into a CLI Script File

Synopsis

`running`

Description

Creates a file named *`running.cli`* that contains CLI commands that would reproduce the current runtime configuration of the switch. This file may be offloaded to an external filesystem to be saved as a backup, or edited, and transferred to other switches as a mechanism to replicate common settings. All non-volatile configuration parameters are included. To instantiate the settings based in this file, type the following command:

 # running.cli

Note: *If RSTP is used, you must first establish RSTP ("span version 2", see page 225), save, and reboot before instantiating settings with the running.cli file.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

File Transfer

Use TFTP to Transfer Files

Synopsis

`tftp <command> <host> <source> <destination>`

where

`command`	is either `get` or `put`.
`host`	is an IP Address type specifying the IP Address of the TFTP Server (see “IP Address” on page 74.)
`source`	is an ASCII Label specifying the path to and name of the source file.
`destination`	is an ASCII Label specifying the path to and name of the destination file.

Description

Invoke the TFTP to transfer files to or from a remote host. If the command specified is *get*, then copy the source file from the remote host to the local file system. If the command specified is *put*, then copy the source file from the local file system to the remote host.

Use FTP to Transfer Files

Synopsis

`ftp <command> <host> <source> <destination> [user] [password]`

where

`command`	is either `get` or `put`.
`host`	is an IP Address type specifying the IP Address of the FTP Server (see “IP Address” on page 74.)
`source`	is an ASCII Label specifying the path to and name of the source file.
`destination`	is an ASCII Label specifying the path to and name of the destination file.
`user`	is an ASCII String specifying the user ID to use for access to the remote host.
`password`	is an ASCII String specifying the password to use for access to the remote host.

Description

Invoke the FTP to transfer files to or from a remote host. If the command specified is `get`, then copy the source file from the remote host to the local filesystem. If the command specified is `put`, then copy the source file from the local filesystem to the remote host. If the username and/or password are not specified, the CLI will prompt for them. The password prompt will not echo the password.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set FTPD User Name

Synopsis

`ftpd userid [userid]`

where

`userid` is an ASCII Label up to 16 characters.

Description

Set the FTP server user name. If no argument is provided, the current value is displayed.

Note: *The default user name is "ftp_user".*

Set FTPD Password

Synopsis

`ftpd password [password]`

Where

`password` is an ASCII Label up to 16 characters.

Description

Set the FTP server password. When entering a password, asterisks are displayed instead of text.

Note: *The default password is "password".*

Set the TFTPD Write Access

Synopsis

`tftpd access [mode]`

where

`mode` is an integer from 1–4 as defined as follows:

1 = Full write access

2 = No write access

3 = Write only if file exists

4 = Write only if file does not exist

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Set the TFTPD write access for the CPC441x server. If no argument is provided, display the current configuration.

Display or Set FTP Server Logging Level

Synopsis

`ftpd log [level]`

where

`level` is a keyword consisting of none, error, or all.

Description

Display or set the current logging state of the FTP server. If no argument is provided, the current value is displayed.

Display or Set the Timeout for TFTPD Transfers

Synopsis

`tftpd timeout [timeout]`

where

`timeout` is a decimal integer representing seconds.

Description

Display or Set the TFTPD server timeout (in seconds). If the packet is not successfully transmitted in this time, the transfer will fail. If no argument is provided, the current value is displayed.

Note: *This parameter only takes effect upon a reboot. Please perform a Save and reboot for this parameter.*

Display or Set the Time to Wait between TFTPD Retries

Synopsis

`tftpd retrytime [time]`

where

`time` is a decimal integer representing seconds.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Display or Set the TFTPD server time to wait (in seconds) between retries. If no argument is provided, the current value is displayed.

Note: *This parameter only takes effect upon a reboot. Please perform a Save and reboot for this parameter.*

Display or Set the Maximum Number of Concurrent TFTPD Connections

Synopsis

```
tftpd sessions [count]
```

where

count is a decimal integer

Description

Display or Set the maximum number of simultaneous clients that may be connected to the TFTPD server at a time. If no argument is provided, the current value is displayed.

Note: *This parameter only takes effect upon a reboot. Please perform a Save and reboot for this parameter.*

Set TFTP Server Logging Level

Synopsis

```
tftpd log [level]
```

where

level is a keyword consisting of none, error, or all.

Description

Display the current logging state of the TFTP server. If no argument is provided, the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Filter Mask Commands

(See “Packet Filtering” on page 311 for more information on packet filters.)

Note: *Packet Filter configurations are not saved in the switch* ***durable*** *file and are not restored upon boot. The user must re-instantiate any User Defined Packet Filters through the use of CLI or Lua scripts invoked by* ***rc.lua****. See “Lua Programming Language” on page 449 and “File System” on page 425.*

Display the Non-System Filter Mask Table

Synopsis

`filter mask show [index]`

where

`index` is an integer between 1 and 16.

Description

Display the filter mask table, excluding entries configured automatically by the system. An optional argument, `index`, may be specified to show only a single entry.

Add a Filter Mask

Synopsis

`filter mask add <index> <ingress> <egress> <filter...>`

where

`index` is a decimal integer in the range 1 to 16.

`ingress` is a 6-bit mask (0-0x3F) that is ‘and-ed’ with the input port number.

`egress` is a 6-bit mask (0-0x3F) that is ‘and-ed’ with the output port number.

`filter` is a bitmask.

Description

Configure an inclusive filter mask. Ingress and egress are port masks to which the filter applies. If the port number(s) is unknown, use the value of 0.

Filters are in the following form:

startbit–endbit=value
or
startbit=value

where startbit and endbit are in the range of 1 to 512. The value can be any hexadecimal string, and will be applied in 4 bit “chunks.” Thus, 1–8=3 would yield a bitmask that looks like this:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

00110011

Bitmasks can also be specified in this form:

startbit1–endbit1,startbit2–endbit2=value

where the user can have any number of startbit and endbit pairs.

Bitmasks can be specified on the Command Line consecutively as well:

1–7=f 8–24=a

In this case, bits 1–7 are assigned to 1, and bits 8–24 are assigned 1010... This would commonly be used to mask off a section of the packet, such as the MAC destination address (1–48=f).

Note: *Filter bits are 1-based (bit 1 is the first bit of the filter mask).*

Delete a Filter Mask

Synopsis

`filter mask delete <index>`

where

`index` is a decimal integer in the range 1 to 8.

Description

Delete the specified filter mask from the filter mask table.

Display the Non-System Filter Rule Table

Synopsis

`filter rule show [index]`

where

`index` is a decimal integer between 1 to 128.

Description

Display the filter rule table, excluding entries configured automatically by the system. An optional argument, `index`, may be specified to show only a single entry.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Add a Filter Rule

Synopsis

`filter rule add <index> <priority> <port> <precedence> <ingress> <egress> <action> <mask> <description> <filter...>`

where

`index`	is a decimal integer between 1 to 128.
`priority`	is a decimal integer in the range 0 to 7.
`port`	is a Port number (see “Port” on page 74).
`precedence`	is a decimal integer in the range 0 to 7.
`ingress`	is a Port number (see “Port” on page 74).
`egress`	is a Port number (see “Port” on page 74).
`action`	is a 7-bit decimal integer.
`mask`	is a decimal integer in the range 1 to 816.
`description`	is an ASCII String of up to 40 characters.
`filter`	is a bitmask.

Description

Configure an inclusive filter rule. The “priority,” “port,” and “precedence” are only used if the action field is set accordingly (see below). The ingress and egress port numbers should only be set if this filter is being set on a specific ingress or egress port. If they are not being used, they should be set to 0.

The action bit is a 7-bit integer with the following values:

Bit 1:	If this bit is set, then the 802.1p priority field is changed to match the specified priority, and send out this packet on the new priority’s CoS Queue.
Bit 2:	If this bit is set, send out this packet on the CoS Queue with the specified priority.
Bit 3:	If this bit is set, the IP TOS Precedence in the IP header is changed to the specified precedence.
Bit 4:	If this bit is set, a copy of the packet is sent to the CPU.
Bit 5:	If this bit is set, the packet is discarded.
Bit 6:	If this bit is set, the packet is sent to the specified port.
Bit 7:	If this bit is set, the packet is sent to the “Mirrored-To” port.

Note: *The action value must be provided as a decimal number. The action bits are not exclusive, which means that to change the 802.1 priority (bit 1) and send the packet out the “Mirrored-To” port (bit 7), the value of the “action” field would be 1000001 in binary, or 65 in decimal.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Filters are in the following form:

startbit–endbit=value
or
startbit=value

where startbit bit and endbit are in the range of 1 to 512. The value can be any hexadecimal string, and will be applied in 4 bit “chunks.” Thus, 1–8=3 would yield a bitmask that looks like this:

00110011

Bitmasks can also be specified in this form:

startbit1–endbit1,startbit2–endbit2=value

where the user can have any number of startbit and endbit pairs. Bitmasks can be specified on the Command Line consecutively as well. In this case, a filter would usually specify a particular MAC or IP address. For example, to specify a destination MAC address of 00:00:00:00:00:02, specify the filter as:

1–48=00000000002.

Note: *Filter bits are 1-based (bit 1 is the first bit of the filter mask).*

Enable or Disable BPDU Filters

Synopsis

`filter bpdu <portlist> [enable]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Display or set the BPDU filter on a group of ports. Enabling the filter will cause frames destined to the IEEE-802 Reserved Bridge Multicast MAC Addresses (01:80:C2:00:00:00 to 01:80:C2:00:00:0F and 01:80:C2:00:00:20 to 01:80:C2:00:00:2F) to be discarded rather than being sent to the on-board CPU. This can relieve the CPU of the processing overhead associated with protocols that utilize these addresses. Note that all packets sent to these special MAC Addresses are discarded with this filter. If it is desired that packets addressed to a subset of these addresses should be sent to the CPU rather than discarded, a packet filter may be used for this purpose (see “Packet Filtering” on page 311).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Delete a Specified Filter Rule

Synopsis

`filter rule delete <index>`

where

`index` is a decimal integer between 1 to 128.

Description

Delete the specified filter rule from the filter rule table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Filtering Database

Flush the Filtering Database

Synopsis

```
fdb flush
```

Description

Remove all learned MAC entries from the filtering database.

Display or Set the Filtering Database Aging Time

Synopsis

```
fdb age [age_time]
```

where

age_time is a decimal integer value between 10 and 1000000 seconds. 300 seconds is the default.

Description

Set the aging time on the filtering database to *age_time* in seconds. If no argument is provided, display the current value.

Display the Dynamic Filtering Database

Synopsis

```
fdb learned [all|<port>|<mac>]
```

where

all is a keyword.

port is a Port number (see “Port” on page 74.)

mac is a MAC Address type (see “MAC Address” on page 74.)

Description

Display entries in the dynamic filtering database. The argument selects the search criteria.

The `all` keyword displays all entries in the dynamic database. The `port` keyword displays all entries in the dynamic database that are valid for the specified port number. The `mac` keyword displays all entries in the dynamic database for the specified MAC address.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Entries displayed from the dynamic database include the MAC Address, and Port. The default setting is `all`.

The output pauses when a full screen is displayed. The user may press ENTER to display the next screen, 'X' to exit the command, or 'Q' to stop displaying the output. If a 'Q' is entered, the database will continue to be searched, and a total line will be printed. This can take some time if the database is large.

Add a Static Multicast Filtering Database Entry

Synopsis

`static mcast add <vid> <mac> [mandatory] [filter]`

where

`vid`	is decimal integer between 1 and 4094.
`mac`	is a MAC Address type (see "MAC Address" on page 74.)
`mandatory`	is a List of Port numbers (see "List" and "Port" on page 74.)
`filter`	is a List of Port numbers (see "List" and "Port" on page 74.)

Description

Add a multicast MAC to the filtering database. The arguments include: a VLAN ID, MAC address, a "mandatory" port list and/or a "filter" port list. The VLAN ID identifies the VLAN for which this entry applies. The MAC address must be a Multicast MAC or the Broadcast MAC. The "mandatory" port list indicates which ports to forward to when a frame destined to the specified MAC and VLAN is received on one of the ingress ports. The "filter" port list indicates which ports not to forward to when a frame destined to the specified MAC and VLAN is received on one of the ingress ports. The "mandatory" and "filter" port lists must be mutually exclusive.

Each port maintains a forwarding rule for each outbound port. The forwarding rule may be any of the following: forward always, forward never, or forward based on a policy defined elsewhere. The multicast MAC entry specifies whether to forward always or filter always for each specified outbound port. If neither of these bits are set for an outbound port, then the frame will be forwarded based on GMRP registrations and/or static "forward all" or "forward unregistered" policies established via the "gmrp all" or "gmrp unregistered" commands.

Note that these static MAC entries take precedence over GMRP registrations and "forward all" or "forward unregistered" policies.

Example:

```
static mcast add 1 01:01:01:01:01:01 1-12 13-26
static mcast add 2 01:01:01:01:01:02 13-18 1-12
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display the Permanent Multicast Filtering Database

Synopsis

`static mcast show [vid] [all|mac <mac_address>]`

where

`all` and *`mac`*	are optional keyword arguments. Default is `all`.
`vid`	is decimal integer between 1 and 4094. Default is 1.
`mac`	is a MAC Address type (see “MAC Address” on page 74.)

Description

Display multicast entries in the permanent filtering database. The `vid` argument selects the VLAN for which the entry applies. The second argument selects the display criteria.

The `all` keyword displays all multicast entries in the permanent database. The `mac` keyword displays the specified MAC address. Since the [all] and [mac] arguments are both optional, you must use the following syntax choices:

```
static mcast show 1 all
```

or

static mcast show 1 mac=01:00:5e:00:20:00

Delete Entries from the Permanent Multicast Filtering Database

Synopsis

`static mcast delete [vid] [all|mac <mac_address>]`

where

`all` and *`mac`*	are optional keyword arguments.
`vid`	is decimal integer between 1 and 4094.
`mac`	is a MAC Address type (see “MAC Address” on page 74.)

Description

Delete multicast entries in the permanent filtering database. The `vid` argument selects the VLAN for which the entry applies. The second argument selects the delete criteria.

The `all` keyword deletes all multicast entries in the permanent database. The `mac` keyword deletes the specified MAC address. Since the [all] and [mac] arguments are both optional, you must use one of the following syntax choices:

```
static mcast delete 1 all
```

or

```
static mcast delete 1 mac=01:00:5e:00:20:00
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Add a Static Unicast Filtering Database Entry

Synopsis

`static ucast add <vid> <mac> [port] [status]`

where

`vid` is decimal integer between 1 and 4094.

`mac` is a MAC Address type (see “MAC Address” on page 74.)

`port` is a Port number (see “Port” on page 74.)

`status` is a string to describe the status of the unicast entry. Valid status strings are:

`permanent` this entry will remain in use after the next reset of the bridge.

`deleteOnReset` this entry will remain in use until the next reset of the bridge.

`deleteOnTimeout` this entry will remain in use until it is aged out.

Description

Add a unicast MAC to the filtering database. The VLAN ID identifies the VLAN for which this entry applies. The MAC address must be a Unicast MAC. The specified port is the port to forward to when a frame destined to the specified MAC and VLAN is received. The status indicates how the system will handle this entry: age it out, make it a permanent static entry, or remove the entry on reset.

The Unicast MAC entry specifies where to forward each specified outbound port and how to handle this entry in the ARL table.

Example:

```
static ucast add 1 66:55:44:33:21:01 1 permanent
static ucast add 13 22:11:44:66:22:01 13 deleteOnTimeout
```

Display the Unicast Filtering Database

Synopsis

`static ucast show`

Description

Display unicast entries in the filtering database.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Delete Entries from the Unicast Filtering Database

Synopsis

`static ucast delete [vid] [mac]`

where

`vid`	is decimal integer between 1 and 4094. Default is 1.
`mac`	is a MAC Address type (see “MAC Address” on page 74.)

Description

Delete unicast entries in the filtering database. The *`vid`* argument selects the VLAN to which the entry applies, and the *`mac`* keyword identifies the specified MAC address.

Set Up Managed Learning for a Port

Synopsis

`learning <portlist> [mode]`

where

`portlist`	is a List of Port numbers (see “List” and “Port” on page 74.)
`mode`	is a string to describe the way a port’s learned packets will be handled. Valid mode strings are:

`learn`	all new addresses are learned.
`flood`	all new addresses are flooded, and statics are switched.
`drop`	no learning of new addresses, frames from unknown sources are dropped. Frames from statically configured addresses are switched.

Description

Set the mode on the ports specified. If no mode is provided, display the current configuration for the specified ports.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

GARP (Generic Attribute Registration Protocol) Management

Set GARP Join Time

Synopsis

garp join <portlist> [join_time]

where

portlist is a List of Port numbers (see “List” and “Port” on page 74.)

join_time is a decimal integer.

Description

Set the Join Timer for the specified list of ports. If no argument is provided, display the current configuration. GARP Join Time is defined and explained in the IEEE 802.1d–1998 specification.

Set GARP Leave Time

Synopsis

garp leave <portlist> [leave_time]

where

portlist is a List of Port numbers (see “List” and “Port” on page 74.)

leave_time is a decimal integer in the range 60 to 20000 in centiseconds. 1000 centiseconds is equal to 10 seconds.

Description

Set the Leave Timer for the specified list of ports. If no argument is provided, display the current configuration. GARP Leave Time is defined and explained in the IEEE 802.1d–1998 specification.

Set GARP LeaveAll Time

Synopsis

garp leaveall <portlist> [leaveall_time]

where

portlist is a List of Port numbers (see “List” and “Port” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

leaveall_time
: is a decimal integer in the range 1000 to 20000 centiseconds. 1000 centiseconds is equal to 10 seconds.

Description

Set the Leave All Timer for the specified list of ports. If no argument is provided, display the current configuration. GARP LeaveAll Time is defined and explained in the IEEE 802.1d–1998 specification.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

GMRP (GARP Multicast Registration Protocol) and Multicast Policy

Enable or Disable GMRP

Synopsis

`gmrp enable [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the CPC441x from using GMRP to build Multicast membership groups. If no argument is provided, display the current configuration.

Enable or Disable GMRP on a Set of Ports

Synopsis

`gmrp set <portlist> [enable]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the operation of GMRP on the selected ports. If no argument is provided, display the current configuration.

Display GMRP Status

Synopsis

`gmrp status <portlist>`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Display the status of GMRP for the specified port(s).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set the Forward All Multicast Port List

Synopsis

`gmrp all forward <vid> [static_ports]`

where

`vid` is decimal integer between 1 and 4094.

`static_ports`
is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Set the forward all multicast policy for a set of ports in the VLAN specified by `vid` to `static` (forward always). All multicast frames will be forwarded to this set of ports and no GMRP registrations for multicast memberships will be accepted on these ports. If the *`static_ports`* argument is not provided, display the current setting.

Display or Set the Port List for which GMRP May Not Register a Forward All Service Requirement

Synopsis

`gmrp all forbidden <vid> [forbidden_ports]`

where

`vid` is decimal integer between 1 and 4094.

`forbidden_ports`
is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Set the list of ports in the VLAN specified by *`vid`* on which ‘GMRP Forward All Service Requirement’ registrations will *not* be accepted. If the *`forbidden_ports`* argument is not provided, display the current setting.

Display or Set the Forward Unregistered Multicast Port List

Synopsis

`gmrp unregistered forward <vid> [static_ports]`

where

`vid` is decimal integer between 1 and 4094.

`static_ports`
is a List of Port numbers (see “List” and “Port” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Set the unregistered multicast forwarding policy for a set of ports in the VLAN specified by *vid* to forward unregistered. All multicast frames for which no specific forwarding information is available will be forwarded to this set of ports. More specific forwarding information may be defined through management by creating a Static Multicast MAC entry or by GMRP. If the *static_ports* argument is not provided, display the current setting.

Display or Set the Port List for which GMRP May Not Register a Forward Unregistered Service Requirement

Synopsis

gmrp unregistered forbidden <vid> [forbidden_ports]

where

vid is decimal integer between 1 and 4094.

forbidden_ports
is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Set the list of ports in the VLAN specified by *vid* on which ‘GMRP Forward Unregistered Service Requirement’ registrations will *not* be accepted. If the *forbidden_ports* argument is not provided, display the current setting.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

GVRP (GARP VLAN Registration Protocol) Management

Enable or Disable GVRP

Synopsis

`gvrp enable [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the CPC441x from using GVRP on all ports. If no argument is provided, display the current configuration.

Enable or Disable GVRP on a Set of Ports

Synopsis

`gvrp set <portlist> [enable]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the operation of GVRP on the selected ports. If no argument is provided, display the current configuration.

Configure GVRP Port Priority

Synopsis

`gvrp priority <portlist> [priority]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`priority` is a decimal integer in the range 0 to 7.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

The default ingress User Priority for this port. Valid values are 0-7. Set the priority for a list of ports. If no argument is provided, the current value is displayed.

Set AdmitAll on a Set of Ports

Synopsis

`gvrp admitall <portlist> [enable]`

where

`portlist` is a List of Port numbers (see "List" and "Port" on page 74.)

`enable` is a Boolean type (See "Boolean" on page 74.)

Description

Display or set `admitall` for a list of ports. The selected ports will either admit all frames (ON), or only VLAN tagged frames (OFF).

Set VLAN Ingress Filter Mode

Synopsis

`gvrp ifilter <portlist> [enable]`

where

`portlist` is a List of Port numbers (see "List" and "Port" on page 74.)

`enable` is a Boolean type (See "Boolean" on page 74.)

Description

Turn ingress filter mode ON or OFF. If ingress filtering is enabled on a port, frames that are received on that port that are classified as being from a VLAN of which the port is not a member, will be discarded. Only frames from VLAN(s) in which the port has membership are allowed. If ingress filtering is disabled, frames are not discarded based on VLAN classification. They are forwarded to all ports that match the VLAN ID of the tagged frame. If `enable` is not specified, display the current configuration.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Associate a PVID with a Set of Ports

Synopsis

`gvrp pvid <portlist> [vid]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`vid` is decimal integer between 1 and 4094.

Description

Display or set the PVID for a list of ports. If no argument is provided, display the current configuration.

Display GVRP Status on a List of Ports

Synopsis

`gvrp status <portlist>`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Display GVRP status for the specified list of ports. (See “Port” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Command History

Display Command History

Synopsis

```
history
```

Description

Display the past 100 commands entered in the CLI. Use the key commands shown in Table 5-8Table 5-8: to retrieve specific commands in the history list.

Table 5-8: History Key-Commands

Control N	Get next line from history list
Control P	Get previous line from history list
ESC <	Move to start of history list
ESC >	Move to end of history list

See “Command Line Editing” on page 76 for a complete list of command line editing commands.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

IGMP Snooping

Enable or Disable IGMP Snooping

Synopsis

`igmp snoop enable [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the operation of IGMP snooping. If `enable` is not specified, the current state will be displayed. (For more information, see“Multicast Filtering” on page 405.)

Enable IGMP Snooping

Synopsis

`igmp on`

Description

Enable the operation of IGMP snooping.

Note: *This command has been retained to provide backward compatibility. The “igmp snoop enable” command is preferred.*

Disable IGMP Snooping

Synopsis

`igmp off`

Description

Disable the operation of IGMP snooping.

Note: *This command has been retained to provide backward compatibility. The “igmp snoop enable” command is preferred.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set the IGMP Snoop Age Timer

Synopsis

`igmp snoop age [age]`

where

`age` is a decimal integer between 30 and 3600 (seconds).

Description

Display or Set the IGMP Query aging time. This is the number of seconds a port will remain in a membership table for a group after it stops sending IGMP Report PDUs for the group. If age is not specified, the current value will be displayed.

Show the Current IGMP Memberships

Synopsis

`igmp snoop show`

Description

Display the current IGMP Snoop memberships. Any Static Mandatory ports are indicated in the display with the letter ‘M’. Static Forbidden ports are indicated by the letter ‘F’. IGMP learned ports are indicated by the letter ‘I’.

Enable IGMP Query Agent on a VLAN

Synopsis

`igmp query enable <vid> [enable]`

where

`vid` is decimal integer between 1 and 4094.

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the IGMP Query Agent on a specified VLAN. If ‘enable’ is not specified, the current state will be displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set the IGMP Query Interval on a VLAN

Synopsis

`igmp query interval <vid> [interval]`

where

`vid`	is decimal integer between 10 and 4094.
`interval`	is a decimal integer (minimum value of 10).

Description

Display or Set the IGMP Query Agent Interval on a specified VLAN. The argument interval specifies the interval at which Query packets are sent when the switch is the IGMP Query Master for the specified VLAN. If interval is not specified, the current value will be displayed.

Display or Set the IGMP Query Expiry Time on a VLAN

Synopsis

`igmp query expiry <vid> [expiry]`

where

`vid`	is decimal integer between 1 and 4094.
`expiry`	is a decimal integer.

Description

Display or Set the IGMP Query Agent Expiry timer on a specified VLAN. The argument expiry specifies the time that a Non-Querier will delay before becoming a Querier unless a Query PDU is received from a lower Source IP Address. If expiry is not specified, the current value will be displayed.

Show the Current IGMP Query Status

Synopsis

`igmp query show`

Description

Display the current IGMP Query status. Each valid Querier entry is displayed along with the Querier/Non-Querier state of each VLAN, the Interval and Expiry times, and the IP Address of the current Querier.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Manage Internet Protocol (IP) Settings

Configure an IP Interface

Synopsis

`ip config <interface> [ip_addr] [net_mask] [vid] [description]`

where

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`ip_addr` and *`Net_Mask`*
are IP Address numbers (See “IP Address” on page 74.)

`vid` is an integer that corresponds to a VLAN Identifier. Once assigned, the VID cannot be changed. In order to change a VID, the interface must be removed and a new interface must be created.

`description` is an ASCII String.

Description

Set the IP address, subnet mask, and description of one of the network interfaces, and associate it with an existing VLAN. The VLAN is identified by its VID. If only the interface is specified, the current configuration will be displayed.

For example, the following command will create an sw1 interface with an IP address 10.10.10.1 and a net mask 255.255.255.0 and will assign it to a default VLAN 1:

```
# ip config sw1 10.10.10.1 255.255.255.0 1
```

Once an interface has been created and assigned to an existing VLAN, additional IP addresses may be assigned to it. This is commonly referred to as IP Multihoming. Additional addresses may be either in the same, or in different subnets. The following command assigns an additional address 10.10.10.2 to a previously created sw1 IP interface:

```
# ip config sw1 10.10.10.2
```

If no net_mask is provided, the existing net_mask is assumed.

The following command assigns an additional address 172.16.1.1 and a net_mask 255.255.240.0 to the sw1 interface:

```
# ip config sw1 172.16.1.1 255.255.240.0
```

The same “ip config” command with no additional arguments may be used to display the settings.

```
# ip config sw1
```

ip config: An IP address must be specified to configure an interface.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Displaying current settings

```
 Interface: sw1
      Name: None
    Status: Active
       MAC: 00:c0:8c:e8:d8:41
       VID: 1
IP address: 10.10.10.1
   Netmask: 255.255.255.0
IP address: 10.10.10.2
   Netmask: 255.255.255.0
IP address: 172.16.1.1
   Netmask: 255.255.240.0
```

Note: *The VLAN must already exist (see "Create a VLAN" on page 250). Also, the subnet mask must be set when the interface is created. Thereafter, when new addresses are added to the interface, if no subnet mask is specified, the existing mask is assumed. Once a VID is assigned to an interface, it cannot be changed without removing the existing interface and creating a new one.*

Assign the Default Gateway

Synopsis

`ip gateway [ip_addr]`

where

`ip_addr` is an IP Address (see "IP Address" on page 74.)

Description

Set the IP address of the CPC441x default gateway to *`ip_addr`*. If no arguments are provided, display the current gateway configuration.

Display Network Statistics

Synopsis

`ip stats <interface>`

where

`interface` is an Interface Description keyword (See "Interface Description" on page 74.)

Description

Display statistics for a network interface, or a group of interfaces if a group is specified. For example, the following command displays all configured sw interfaces:

```
# ip stats sw
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

In the example, the single network interface has been assigned three different IP addresses:

```
 Interface: sw1
      Name: None
    Status: Active
       MAC: 00:c0:8c:e8:d8:41
       VID: 1
IP address: 10.10.10.1
   Netmask: 255.255.255.0
IP address: 10.10.10.2
   Netmask: 255.255.255.0
IP address: 172.16.1.1
   Netmask: 255.255.240.0
```

Delete an Interface or an IP Address Associated with an Interface

Synopsis

`ip delete <interface> [ip_addr]`

where

`interface` is an Interface Description keyword (see “Interface Description” on page 74.)

`ip_addr` is an IP Address to be removed (see “IP Address” on page 74.)

Description

If an *`ip_addr`* is provided, then this command removes the specified IP address. If no *`ip_addr`* is specified, then this command removes the specified interface with all of its associated IP addresses.

For example, the following command removes the 172.16.1.1 IP address from the sw1 interface:

```
# ip delete sw1 172.16.1.1
```

The following command removes the sw1 interface and all of its associated IP addresses:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

ip delete sw1Configure Forwarding

Synopsis

ip forward [enable]

where

enable is a Boolean type (see “Boolean” on page 74.)

Description

Enable or disable forwarding of datagrams received, but addressed to a host on a different network. The CPC441x must be configured to have an interface to both the source and destination networks. If no arguments are provided, display the current forward status.

Configure Default TTL (Time to Live)

Synopsis

ip ttl [value]

where

value is an integer value between 1 and 255.

Description

Set the default TTL value sent with frames transmitted by the CPC441x. If no arguments are provided, display the current TTL value.

Display ARP Table

Synopsis

ip arp display [ip_address]

where

ip_addr is an IP Address type (see “IP Address” on page 74.)

Description

Display the ARP Table entry for the specified IP Address. If no parameter is provided, display the entire table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Add Entry to ARP Table

Synopsis

`ip arp add <ip_address> <mac_address> [published]`

where

`ip_address` is an IP Address type (see “IP Address” on page 74.)

`mac_address` is a MAC Address type (see “MAC Address” on page 74.)

`published` is a Boolean type (See “Boolean” on page 74.)

Description

Add or update an entry for the IP Address associating the IP Address with the specified MAC Address. If the parameter *`published`* is set to TRUE, announce (via an ARP Reply to the network), the MAC Address / IP Address pairing.

Remove Entry from ARP Table

Synopsis

`ip arp remove <ip_address>`

where

`ip_address` is an IP Address type (see “IP Address” on page 74.)

Description

Remove the ARP entry for the specified IP Address.

Configure ARP Verify

In normal operation, ARP entries are removed every 20 minutes. This allows the switch to relearn Ethernet addresses that may have changed (for hosts that do not send a gratuitous ARP). Removing the ARP entry also causes the deletion of any L2 and L3 information. Under normal circumstances this isn't a problem since the information will be relearned. However, if there is a great deal of L3 traffic associated with this entry, it can place a significant burden on the switch to reacquire and install the L3 information.

An alternative to deleting the ARP information every 20 minutes is to instead verify it. If the information is unchanged, the L2 & L3 information is not removed. This behavior can be enabled with this command.

Without the optional on/off keywords, the current status will be displayed. When enabled, ARP entries will be verified approximately 2 minutes prior to being removed. If there is no response to the ARP request, the entry will be removed at the normal timeout duration.

Note that using this feature means that entries may remain in the ARP, L2 and L3 tables indefinitely. L2 aging will also remove L2 and L3 entries if the station is inactive.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Synopsis

`ip arp verify [mode]`

where

`mode` is a Boolean type (See “Boolean” on page 74.)

Description

Used to set up ARP verify feature as described above. If the mode argument is omitted, this command will return the current verify setting.

`published` is a Boolean type (See “Boolean” on page 74.)

Flush ARP Table Entries

Synopsis

`ip arp flush`

Description

Remove all entries from the ARP table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Intelligent Platform Management Interface (IPMI): Field Replaceable Unit (FRU)

The following FRU commands allow the user to modify and inspect any of the FRU objects. If an object value is modified, it must be saved in the peripheral management controller (PM) non-volatile storage using the appropriate apply command. The apply command is available at two of the FRU group levels (board and product groups).

Execution of the `apply` command at either of these group levels will send the FRU data to the PM hardware to be updated (this may take a few seconds).

Each of the FRU objects supports a show command. The show commands transfer the current FRU values from NVRAM to DRAM prior to displaying them. This process over-writes any values in DRAM that have not been saved with the apply command. If a FRU object is being modified, do not execute the show command before you execute the apply command, or your modified values will be lost.

The Header FRU Info Area is not writable. The Board Info FRU Area is writable, but it should not normally changed by the OEM user of the switch. This area is configured in the manufacturing process at Performance Technologies. The original Performance Technologies manufacturing information will be lost if this area is modified. The OEM user of the switch may utilize the Product FRU Info Area for OEM information.

The FRU data managed by the switch is defined in the document, “IPMI - Platform Management FRU Storage Definition, V 1.0”, by Intel, Hewlett-Packard, NEC, Dell.

Display FRU Information

Synopsis

```
ipmi fru show
```

Description

This command will display all appropriate FRU MIB information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Values in the FRU Common Header Area Information

The Common Header Info FRU Area is set at the factory with offsets into the other FRU groups. This area is not writable.

Display FRU Common Header Information

Synopsis

```
ipmi fru header show
```

Description

This command will display all appropriate FRU Common Header MIB information. The FRU Common Header provides offsets into the other FRU areas.

Values in the FRU Board Area Information

The Board Info FRU Area is set at the factory with board product information. It is not typically changed by the OEM user of the switch.

Display or Set FRU Board Area Format Version Value

Synopsis

```
ipmi fru board version [value]
```

where

value is the value the user wants this object to store.

Description

This function will display or configure the Board Area Format Version object. This object should never be changed by the user.

Display the FRU Board Area Length Value

Synopsis

```
ipmi fru board length
```

Description

This function will display Board Area Length object. The Board Info Area Length defines the size of the Board Area structure in multiples of 8 bytes.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set FRU Board Area Language Code Value

Synopsis

`ipmi fru board langcode [value]`

where

`value` is the value the user wants this object to store.

Description

This function will configure Product Language Code object. en(25) is the code for English.

Display or Set FRU Board Area Manufacturing Date Value

Synopsis

`ipmi fru board mfgdate [value]`

where

`value` is the value the user wants this object to store.

Description

This function will configure Board Manufacture Date object. The date and time of Manufacturing is given in number of minutes since 0:00 hours 1/1/96.

Display or Set FRU Board Area Manufacturer Name Value

Synopsis

`ipmi fru board mfgname [value]`

where

`value` is the value the user wants this object to store.

Description

This function will configure Board Manufacturer’s name.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set FRU Board Area Product Name Value

Synopsis

`ipmi fru board productname [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure the Product Name object.

Display or Set FRU Board Area Serial Number Value

Synopsis

`ipmi fru board serialnumber [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure the Product Serial Number object.

Display or Set FRU Board Area Part Number Value

Synopsis

`ipmi fru board partnumber [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure the Board Part Number object.

Display or Set FRU Board Area File ID Value

Synopsis

`ipmi fru board frufileid [value]`

where

`value` is the value the user wants this object to store.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

This function will configure Product FRU File ID object. The FRU File version field is a pre-defined field provided as a manufacturing aid for verifying the file that was used to load the FRU information during manufacture or field update. The content is manufacturer-specific. This field is also provided in the Product Info Area.

Display or Set FRU Board Area Custom Manufacturing Area 1 Value

Synopsis

```
ipmi fru board customone [value]
```

where

value is the value the user wants this object to store.

Description

This function will display or configure one of three Board Area Custom Manufacturing objects. These objects are strings that identify additional manufacturing information for the board.

Display or Set FRU Board Area Custom Manufacturing Area 2 Value

Synopsis

```
ipmi fru board customtwo [value]
```

where

value is the value the user wants this object to store.

Description

This function will display or configure one of three Board Area Custom Manufacturing object. These objects are strings that identify additional manufacturing information for the board.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set FRU Board Area Custom Manufacturing Area 3 Value

Synopsis

```
ipmi fru board customthree [value]
```

where

value is the value the user wants this object to store.

Description

This function will display or configure one of three Board Area Custom Manufacturing object. These objects are strings that identify additional manufacturing information for the board.

Set Values in the FRU Board Information Area

Synopsis

```
ipmi fru board apply
```

Description

The `apply` command is used to have all the modified FRU data sent to the hardware.This command must be issued after changing any of the Board Area FRU information.

Display FRU Board Information

Synopsis

```
ipmi fru board show
```

Description

This command will display all appropriate FRU Board Info Area MIB information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Values in the FRU Product Area Information

The Product Info FRU Area is available to the OEM user of the switch to allow for storage of OEM product information.

Display or Set FRU Product Area Format Version Value

Synopsis

```
ipmi fru product prdversion [value]
```

where

value is the value the user wants this object to store.

Description

This function will display or configure the Product Area Format Version object.

Display or Set FRU Product Area Language Code Value

Synopsis

```
ipmi fru product langcode [value]
```

where

value is the value the user wants this object to store.

Description

This function will configure Product Area Language Code object. “en(25)” is the code for English.

Display the FRU Product Area Length Value

Synopsis

```
ipmi fru product length
```

Description

This function will display Product Area Length object. The Product Info Area Length defines the size of the Product Area structure in multiples of 8 bytes.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set FRU Product Area Manufacturer Name Value

Synopsis

`ipmi fru product mfgname [value]`

where

`value` is the value the user wants this object to store.

Description

This function will configure Product Area Manufacturer's name.

Display or Set FRU Product Area Product Name Value

Synopsis

`ipmi fru product productname [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure the Product Area Product Name object.

Display or Set FRU Product Area Model Number Value

Synopsis

`ipmi fru product modelnumber [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure the Product Area Model Number object.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set FRU Product Area Product Version Value

Synopsis

`ipmi fru product version [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure the Product Area Version object.

Display or Set FRU Product Area Serial Number Value

Synopsis

`ipmi fru product serialnumber [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure the Product Area Serial Number object.

Display or Set FRU Product Area Asset Tag Value

Synopsis

`ipmi fru product assettag [value]`

where

`value` is the value the user wants this object to store.

Description

This function will configure the Product Area Asset Tag. The value will be stored internally as in type/length byte format.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set FRU Product Area File ID Value

Synopsis

`ipmi fru product frufileid [value]`

where

`value` is the value the user wants this object to store.

Description

This function will configure Product FRU File ID object. The FRU File version field is a pre-defined field provided as a manufacturing aid for verifying the file that was used to load the FRU information during manufacture or field update. The content is manufacturer-specific. This field is also provided in the Product Info Area.

Display or Set FRU Product Area Custom Product Info 1 Value

Synopsis

`ipmi fru product customone [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure one of three Product Area Custom Manufacturing object. These objects are strings that identify additional product information for the board.

Display or Set FRU Product Area Custom Product Info 2 Value

Synopsis

`ipmi fru product customtwo [value]`

where

`value` is the value the user wants this object to store.

Description

This function will display or configure one of three Product Area Custom Manufacturing object. These objects are strings that identify additional product information for the board.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set FRU Product Area Custom Product Info 3 Value

Synopsis

```
ipmi fru product customthree [value]
```

where

value is the value the user wants this object to store.

Description

This function will display or configure one of three Product Area Custom Manufacturing object. These objects are strings that identify additional product information for the board.

Set Values in the FRU Product Information Area

Synopsis

```
ipmi fru product apply
```

Description

The `apply` command is used to have all the modified FRU Product Area data sent to the hardware.This command must be issued after changing any of the Product Area FRU information.

Display FRU Product Area Information

Synopsis

```
ipmi fru board show
```

Description

This command will display all appropriate FRU Product Info Area MIB information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Intelligent Platform Management Interface (IPMI): Peripheral Management (PM) Controller

Display the Geographic Address Seen by the PM Controller

Synopsis

```
ipmi pm geoaddress
```

Description

This function will display the CompactPCI Geographic Address bits (GA0-GA4).

Display the GUID Value of the PM Controller

Synopsis

```
ipmi pm guid
```

Description

This function will display the PM Globally Unique Identifier value. The GUID value is established in the manufacturing process and is unique for every PM.

Reset the PM Controller

Synopsis

```
ipmi pm pmreset
```

Description

This function will reset the PM controller. A reset is necessary after loading a new PM program into the PM micro-controller.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Reprogram the PM Controller Firmware

Synopsis

ipmi pm progfile [filename]

where

filename is the name of the Hex-record format PM Object file.

Description

This command is used to upgrade the PM firmware. The file will need to be in flash on the board. The ‘filename’ is the name of the ‘Hex-record’ file that contains the new PM micro-controller program. If PM program update is needed, instructions will be included in release notes provided by Performance Technologies.

Reset the PM Controller IPMI Transaction Statistics

Synopsis

ipmi pm statsclear

Description

This function will reset the IPMI transaction statistics maintained by PM controller. The PM controller maintains statistics on IPMI bus command transactions including; command counts, collisions, errors, etc.

Display the Firmware Version Information of the PM Controller

Synopsis

ipmi pm version

Description

This function will display the PM firmware version information.

Display PM Information

Synopsis

ipmi pm show

Description

This command will display PM information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display IPMI Transaction Statistics Information

Synopsis

```
ipmi pm statsshow
```

Description

This command will display the PM Statistics MIB information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Link Aggregation

Link Aggregation allows two or more physical ports to be aggregated together forming a Link Aggregation Group, such that a MAC Client can treat the Link Aggregation Group as if it were a single link. Performance Technologies' Link Aggregation implementation fully conforms to the IEEE 802.3ad specification. This section assumes familiarity with this specification. Also See "Link Aggregation" on page 385 for more information.

Enable or Disable Link Aggregation

Synopsis

`lag enable [enable]`

where

`enable` is a Boolean type (see "Boolean" on page 74.)

Description

Enable or disable link aggregation on the CPC441x. If no argument is provided, display the current value.

Display Link Aggregation ID

Synopsis

`lag show ID`

Description

Displays the Link Aggregation Group Identifier for both the partner and the actor, as in this example:

```
*******************************************************************************
                    [(actor LAG ID), (partner LAG ID)
-------------------------------------------------------------------------------
P# A# [(Prio, MAC, key ,pr,P # ), (Prio,MAC,key ,pr,P # )]
-------------------------------------------------------------------------------
01 01 [(8000,00-03-31-01-00-02,0001,00,0000), (8000,00-00-00-00-00-00,0001,00,0000)]
02 01 [(8000,00-03-31-01-00-02,0001,00,0000), (8000,00-c0-8c-08-60-04,0001,00,0000)]
*******************************************************************************
```

The LAG ID comprises System Priority, System MAC Address, Key, Port Priority, and Port Number.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Link Aggregation States

Synopsis

`lag show states`

Description

Displays states of various Link Aggregation state machines. There are three state machines for each aggregation port: Receive, Transmit, and Mux. The `lag show states` command also displays the state of the Selection logic, which can be either SELECTED if an aggregation port has selected its aggregator, or UNSELECTED. Following is an example of a lag show states display:

```
*****************************************************************
                    LACP State Machines: ver 01
-----------------------------------------------------------------
Port  Receive    Transmit     Selection  Mux        LACP  Ag  CD
-----------------------------------------------------------------
01    CURRENT    PERIODIC_TX  SELECTED   COL_DISTR  YES   01  1
02    CURRENT    PERIODIC_TX  SELECTED   COL_DISTR  YES   01  1
03    DEFAULTED  PERIODIC_TX  SELECTED   COL_DISTR  YES   03  1
*****************************************************************
```

`Port` is the aggregation port number.

`Receive` shows the state of the Receive State Machine, which can be one of the following: INITIALIZE, PORT_DISABLE, EXPIRED, LACP_DISABLED, DEFAULTED, or CURRENT. Refer to the IEEE 802.3ad specification for more information. In the example presented above, ports 1 and 2 are attached to aggregator 1 and are receiving LACPDUs from the link partner. Therefore, the Receive Machine is in a CURRENT state. Port 3 is attached to its own aggregator and since it does not receive Link Aggregation Protocol Data Units (LACPDUs), it has transitioned into a DEFAULTED state in which it uses administrative defaults rather than the information communicated by the protocol partner.

`Transmit` shows the state of the Transmit State Machine. This state machine is responsible for periodic LACPDU transmission on all ports that have Link Aggregation Protocol enabled. Remember that ports that are in Half Duplex mode, or that have not established link, will not participate in the LACPDU exchange. The allowed states are NO_PERIODIC or PERIODIC_TX. The parameter Partner_Oper_Port_State.LACP_Timeout will determine whether the transmission is enabled at fast or slow transmission rate.

`Selection` shows the state of the selection logic for the port: SELECTED if a port selected its aggregator, or UNSELECTED otherwise.

`Mux` displays the state of the MUX State Machine. This state machine can be in one of the following states: DETACHED, WAITING, ATTACHED, or COLL_DIST (collecting/distributing).

`LACP` shows whether Link Aggregation Control Protocol is enabled or disabled on the particular port.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Ag	shows the aggregator that has been selected by the aggregation port.
CD	indicates the Collecting/Distributing state of the hardware. “1” means Collecting/Distributing, “0" means that hardware is currently programmed not to accept user traffic.

Display Aggregator Configuration

Synopsis

lag show agg

Description

Displays information contained in the Aggregator Configuration Table, as in the following example:

```
*******************************************************************************
                    LAC Aggregator Information
-------------------------------------------------------------------------------
P#  MAC               ID   Indv Key  PMAC                PK  Ready/N
-------------------------------------------------------------------------------
01  00:03:31:01:00:12  001  NO   01   00:00:00:00:00:0001  YES  /YES
02  00:03:31:01:00:14  002  NO   01   00:c0:8c:08:60:0401  YES  /YES
03  00:03:31:01:00:16  003  YES  01   00:c0:8c:08:60:0401  YES  /YES
*******************************************************************************
```

P#	is the aggregator number.
MAC	is the Actor’s MAC address assigned to a particular aggregator.
ID	is an Aggregator’s ID.
Indv	is a Boolean which indicates whether the port is individual (YES) or aggregatable (NO).
Key	is a port’s operational Key.
PMAC	is a Partner’s MAC address.
PK	is a partner’s operational key.
Ready/N	is a state of the Ready and Ready_N used by the Selection logic.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display LAC Port Information

Synopsis

`lag show port`

Description

Displays information contained in the LAC (Link Aggregation Control) Port Table, as in the following example:

```
*********************************************************************************************
                    LAC Port Information
---------------------------------------------------------------------------------------------
P#  PP#  NTT  MAC               Key  Pri  State     PState     Move  Lnk  Dpx   Spd
---------------------------------------------------------------------------------------------
01  001  NO   00:03:31:01:00:2c  001  128  1011 1110 0001 1110  NO    Up   Full  100
02  002  NO   00:03:31:01:00:2d  001  128  1011 1100 1011 1100  NO    Up   Full  100
03  003  NO   00:03:31:01:00:2e  001  128  1011 1100 1011 1100  NO    Up   Full  100
*********************************************************************************************
```

`P#`	is the actor's port number.
`PP#`	is the partner's port number.
`NTT`	shows the state of the Need To Transmit variable.
`MAC`	is the Actor's MAC address assigned to the aggregation port.
`Key`	is the Actor's operational key.
`Pri`	is the Port's Priority.
`State`	is the Actor's operational state. The eight bits represent the following set of eight variables: LACP_Activity, LACP_Timeout, Aggregation, Synchronization, Collecting, Distributing, Defaulted, Expired.
`Pstate`	is the Partner's operational state. The eight bits represent the following set of eight variables: LACP_Activity, LACP_Timeout, Aggregation, Synchronization, Collecting, Distributing, Defaulted, Expired.
`Moved`	shows whether the port has been moved; if "Yes," then the LACPDU previously received on a different port has now been received on this port.
`Lnk`	shows the state of the aggregation port link state (Up/Down)
`Dpx`	shows duplex status (Full/Half).
`Spd`	shows port's speed in Mb/s.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display LAC Aggregator Port Information

Synopsis

`lag show agg_port`

Description

Displays information in the LAC (Link Aggregator Control) Aggregator Port Information table, as in the following example:

```
*********************************************************************************
                    LAC Aggregator Port Information
---------------------------------------------------------------------------------
P#   AKey   PKey   Loop   Ind   APort   Pbits                          Ports
---------------------------------------------------------------------------------
01   0001   0001   NO     NO    0001    00 00000000 00000000 00000011   1,2
02   0001   0001   NO     NO    0001    00 00000000 00000000 00000000   1,2
*********************************************************************************
```

`P#`	identifies a port number.
`Akey`	is the actor's operational key.
`Pkey`	is the partner's operational key.
`Loop`	identifies whether this port is connected to another port on the same switch.
`Ind`	is a Boolean identifying whether the port is Individual (NO) or aggregatable (YES).
`Aport`	identifies an aggregator to which this port is attached.
`Pbits`	is an 8-bit mask identifying ports which form a trunk group.
`Ports`	identifies ports that selected the same aggregator (forming an aggregation group).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Link Aggregation Timers

Synopsis

`lag show timers`

Description

Displays the settings of the Link Aggregation timers. There is a set of timers running for each port. Following is an example:

```
*********************************************************************************************
                     LACP Timers
---------------------------------------------------------------------------------------------
Port   Cur_while   Wait_while   tV_sched   periodic_t   NTT   HCT
---------------------------------------------------------------------------------------------
01     84 (90) A   00 (02) N    01 (01) A  14 (30) A    NO    1
02     84 (90) A   00 (02) N    01 (01) A  14 (30) A    NO    1
03     84 (90) A   00 (02) N    01 (01) A  14 (30) A    NO    1
*********************************************************************************************
```

`Port` identifies the port number.

`Cur_while` Current While Timer is used to detect whether received protocol information has expired. This timer can be set to either Short Timeout (3 s) or Long Timeout (90 s). The Timer Value in parenthesis (90) identifies the Timeout Time to which the Current While Timer is set. The number in front of it shows the current state of the timer. If this number decrements to zero before the LACPDU is received on the port, the protocol information on the port expires. The letters A/N indicate whether this timer is currently active (A) or not active (N).

`Wait_while` Wait While Timer provides hysteresis (i.e., a pause) before performing an aggregation change, to allow all links that will join this aggregation to do so. The value in parenthesis (2) specifies the Timeout Time to which the Wait While Timer is set. The number in front of it shows the current state of the timer. The letters A/N indicate whether this timer is currently active (A) or not active (N).

`Tx_sched` TX Scheduler Timer is used to delay transmission after receiving a Need To Transfer (NTT) signal, which allows for a brief period of synchronous completion of desired changes to the aggregation hardware states, reducing the total number of messages transmitted. The value in parenthesis (1) specifies the Timeout Time to which the TX Scheduler Timer is set. The number in front of it shows the current state of the timer. The letters A/N indicate whether this timer is currently active (A) or not active (N).

`Periodic_t` Periodic Transmission Counter is used to generate periodic LACPDU transmissions. This counter may be set to either Fast Periodic (1 second) or Slow Periodic (30 seconds). The value in parenthesis (30) specifies the Timeout Time to which the TX Scheduler Timer is set. The number in front of it shows the current state of the timer. The letters A/N indicate whether this timer is currently active (A) or not active (N).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

NTT	Need To Transfer shows whether protocol transmissions are required. NTT is set to TRUE if the Partner's view of the Actor's operational parameters is not up to date.
HTC	Hold Count. IEEE 802.3ad allows for up to three LACPDUs to be sent out within the Periodic Timeout Time. If more LACPDUs need to be sent, the Hold Count is incremented to ensure that the LACPDU will be sent with the next transmission opportunity.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Link Aggregation Statistics

Synopsis

`lag show stats`

Description

Displays Link Aggregation Statistics, as in the following example:

```
*********************************************************************************
                    LAC Port Statistics
---------------------------------------------------------------------------------
P#  PL  TxPDU  RxPDU  RxIllg  RxUnkn  RxMrk  RxMrs  hold  moved  ChangeCt  TransCt
---------------------------------------------------------------------------------
01  UU  000027 000024 000000  000000  000000 000000 0001  0000   00000000  00000001
02  UU  000027 000025 000000  000000  000000 000000 0001  0000   00000000  00000001
03  UU  000027 000025 000000  000000  000000 000000 0001  0000   00000000  00000001
*********************************************************************************
```

`P#`	is a port number.
`PL`	shows whether port (P) and LACP Protocol (L) are Up (U) or Down (D). For example, UU indicates that the port is Up and the LACP protocol on the port is Up.
`TxPDU`	shows the number of LACPDUs sent on this port.
`RxPDU`	shows the number of valid LACPDUs received on this port.
`RxIllg`	shows the number of frames received that carry the Slow Protocol Ethernet Type value, but contain a badly formed PDU or illegal value of Protocol Subtype.
`RxUnkn`	shows the number of frames received that either carry the Slow Protocol Ethernet Type value but contain an unknown PDU, or are addressed to the Slow Protocol Ethernet group MAC Address, but do not carry the Slow Protocol Ethernet Type.
`RxMrk`	shows the number of valid Marker PDUs received on this port.
`RxMrs`	shows the number of valid Marker Response PDUs received on this port.
`hold`	is set to 1 if there is an LACPDU waiting for the next transmission opportunity.
`moved`	shows whether the port has been moved.
`ChangeCt`	shows how many times protocol partner transitioned out of sync.
`TransCt`	shows how many times the actor synchronized with the protocol partner.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Trunk Group Information

Synopsis

`lag show trunks`

Description

Displays Trunk Group Table information. The CPC441x switch hardware implements a Port Trunking feature which is utilized by the Link Aggregation Algorithm. When a new aggregation group containing more than one port is formed, it is assigned to a Trunk Group. When ports leave an aggregation group resulting in a group with fewer than two ports, the Trunk Group is placed into the free pool. The lag show trunks command shows how the Trunk Groups are assigned. The CPC441x hardware supports up to six trunk groups. The display of the lag show trunks looks like the following:

```
**************************************************************************
Total trunks = 6, Trunks left (not used) = 5
**************************************************************************
Trunk #   In Use   RTAG   AGG_NO
--------------------------------------------------------------------------
00        YES      0x01   1
01        NO       0x00   0
02        NO       0x00   0
03        NO       0x00   0
04        NO       0x00   0
05        NO       0x00   0
--------------------------------------------------------------------------
```

`Total trunks` shows the total number of Trunk Groups supported by the hardware.

`Trunks left` shows the number of Trunk Groups left in the free pool.

`Trunk #` is the Trunk Group number (0-5).

`In Use` is a Boolean indicating whether this trunk group is currently being used by the Link Aggregation Algorithm.

`RTAG` is the distribution rule programmed into this Trunk Group (see “Assign Link Aggregation Distribution Criteria” on page 162).

`AGG_NO` identifies the aggregator associated with this Trunk Group.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Trunk Group Mapping

Synopsis

`lag show atgm`

Description

Displays the Aggregator to Trunk Group Mapping (ATGM) table. The CPC441x has as many aggregators as there are aggregation ports. Each aggregation port can be connected to its own aggregator, or can join another aggregation through a different aggregator. Aggregators connected to more than one aggregation port map to Trunk Groups. The CPC441x has 26 aggregation ports and 26 aggregators but only six Trunk Groups. This limitation is dictated by the underlying hardware. The lag show atgm command shows the mapping between the aggregators and the Trunk Groups, which may look like the following:

```
**************************************************************************
                    Aggregator to Trunk Group Mapping table (ATGM)
**************************************************************************
AG #   TGID   RTAG   SelPort   Port List
--------------------------------------------------------------------------
01     000    01     00000001  0000000f
02     255    00     00000002  00000000
03     255    00     00000004  00000000
04     255    00     00000008  00000000
05     255    00     00000010  00000010
**************************************************************************
```

`AG #` is the aggregator number (1 - 26).

`TGID` is the Trunk Group ID (0 - 5, or 255 if unassigned).

`RTAG` is the distribution rule programmed into this Trunk Group (see “Assign Link Aggregation Distribution Criteria” on page 162).

`SelPort` is a bitmask in hexadecimal notation that specifies a port selected within this Trunk Group to handle IEEE PDUs.

`Port List` is a list of all the aggregation ports (bitmask in Hexadecimal notation) attached to this aggregator.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Assign Link Aggregation Distribution Criteria

Synopsis

`lag config rtag <portlist> [distribution]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`distribution` is an ASCII String, consisting of one of the following:

SrcMAC (1)	packets are distributed to a destination port based on the last three bits of the Source MAC Address.
DestMAC (2)	packets are distributed to a destination port based on the last three bits of the Destination MAC Address.
SrcXORDestMAC (3)	packets are distributed to a destination port based on the result of logcially XORing the last three bits of the Source MAC address with the last three bits of the Destination MAC address.
SrcIP (4)	packets are distributed to a destination port based on the last three bits of the Source IP address.
DestIP (5)	packets are distributed to a destination port based on the last three bits of the Destination IP address.
SrcXORDestIP (6)	packets are distributed to a destination port based on the result of logically XORing the last three bits of the Source IP address with the last three bits of the Destination IP address.

Description

Assigns a distribution rule (“rtag”) to a Trunk Group specifying the criteria for distributing Ethernet traffic among the ports in the trunk group. If no argument is specified, display distribution values assigned to all ports.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Ports as Aggregatable

Synopsis

`lag config aggr <portlist> [enable]`

where

`portlist`	is a List of Port numbers (see “List” and “Port” on page 74.)
`enable`	is a Boolean type (on = aggregatable, off = individual) (See “Boolean” on page 74.)

Description

Ports set as individual will not aggregate, regardless of any other settings. Setting ports as aggregatable does not necessarily mean they will aggregate. In order for ports to aggregate they must be assigned the same administrative key, they must be configured to full duplex, and they must have the same speed; they must also have similarly configured link partners. By default, all ports are set as aggregatable.

Assign an Actor System Priority Value

Synopsis

`lag config actor spri <portlist> [spri_value]`

where

`portlist`	is a List of Port numbers (see “List” and “Port” on page 74.)
`spri_value`	is a 2-byte value indicating the priority value associated with the actor’s System ID. The system priority can be set to a decimal value in the range 1 - 65535. The default is 32768.

Description

Assigns a priority value to an actor’s system ID. The following command will assign actor’s system priority 100 on ports 4-8:

```
# lag config actor spri 4-8 100
```

If a priority value is not specified, display the current system priority.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Assign an Actor Key Value

Synopsis

`lag config actor akey <portlist> [akey]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`akey` is an integer between 1 and 26.

Description

Akey is a value assigned to the specified actor port(s). An aggregation port and its associated aggregator always have the same key, i.e., a key assigned to port 1 becomes the key for aggregator 1, etc. If no argument is specified, display administrative keys assigned to all specified ports. By factory default, ports 1-8 are assigned akey = 1, ports 9-16 are assigned akey = 2, ports 17-24 are assigned akey = 3 and ports 25-26 are assigned akey = 4.

For example, the following command will assign an akey value of 10 to ports 4-8:

```
# lag config actor akey 4-8 10
```

Set Maximum Delay

Synopsis

`lag config actor delay`

Description

Delay value is the maximum delay, in tens of microseconds, that may be imposed by the Frame Collector between receiving a frame and either delivering the frame to its MAC Client or discarding the frame. The value is read only.

Note: *A setting of 65535 indicates this feature is disabled.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set a Port Priority

Synopsis

`lag config actor ppri <portlist> [ppri]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`ppri` is an 8-bit value specifying port priority. A priority value can range from 1 to 255; 128 is the factory default.

Description

This command assigns a priority value in the range 1 - 255 to a specified port or ports. The priority value assigned to a port is used to converge dynamic Key changes. If no optional argument is specified, display port priorities for all specified ports.

Display or Set Link Aggregation States

Synopsis

`lag config actor state <portlist> [state]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`state` (in hexadecimal notation) is an eight-bit value describing the state of the aggregator state machines. The first bit corresponds to bit 0 of the Actor_State (LACP_Activity), the second bit corresponds to bit 1 (LACP_Timeout), the third bit corresponds to bit 2 (Aggregation), the fourth bit corresponds to bit 3 (Synchronization), the fifth bit corresponds to bit 4 (Collecting), the sixth bit corresponds to bit 5 (Distributing), the seventh bit corresponds to bit 6 (Defaulted), and the eighth bit corresponds to bit 7 (Expired).

Description

This command allows you to alter the behavior of the Link Aggregation State Machines by setting various states. `State` corresponds to the administrative value of Actor_State as transmitted by the Actor in LACPDUs. The first most significant bit corresponds to the Actor_State (LACP_Activity), the second most significant bit corresponds to LACP_Timeout, the third bit corresponds to Aggregation, the fourth bit corresponds to Synchronization, the fifth bit corresponds to Collecting, the sixth bit corresponds to Distributing, the seventh bit corresponds to Defaulted, and the eighth bit corresponds to Expired.

For example, the following command will disable Link Aggregation on port 1:

```
# lag config actor state 1 72
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The default administrative value of the port state is set to 0xf2. By setting it to 0x72, we cleared the most significant bit (LACP_Activity). If no state is specified, display state for all specified ports.

Set Timeout

Synopsis

`lag config actor timeout <portlist> [timeout]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`timeout` is a keyword, either short (3 seconds) or long (90 seconds).

Description

`timeout <short | long>` is a value assigned to the Actor_State (LACP_Timeout). This is the same value assigned in the state command. The LACP_Timeout controls the current_while timer. When an LACPDU is received on a port, the current_while timer is started with a Short_Timeout_Time (3 seconds) or Long_Timeout_Time (90 seconds), depending upon the Actor's operational value of the LACP_Timeout. If no LACPDU is received before the current_while timer expires, the Receive state machine transitions into the EXPIRED and then into the DEFAULTED state, at which time all partner parameters are overwritten with administratively configured values (defaults). If a timeout value (short/long) is not specified, display the current value for the specified ports.

Configure Partner ID

Synopsis

`lag config partner id <portlist> [mac]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`mac` is a MAC Address (see “MAC Address” on page 74.)

Description

This command administratively sets the partner’s MAC address. By default, all partner MAC addresses are assigned to 00:00:00:00:00:00. When the actor (local switch) and the partner start exchanging Link Aggregation Protocol Data Units (LACPDUs), the partner’s default MAC address will be replaced with a real MAC address communicated inside the LACPDU packet. If optional arguments are not specified, display current MAC addresses assigned to all specified Partner ports.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Assign a Partner Key Value

Synopsis

`lag config partner key <portlist> [key]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`key` is an integer between 1 and 65535.

Description

This command assigns an administrative key to the protocol partner. The factory default partner keys are 1 for port 1, 2 for port 2, etc. This insures that ports will not aggregate unless LACPDUs are exchanged between the actor (the local switch) and the protocol partner. When the exchange of Link Protocol information occurs, the locally set partner keys will be replaced with the real partner keys assigned on the other switch. This is further explained in “Link Aggregation” on page 385, and also in the IEEE 802.3ad specification.

Assign a Partner Port Value

Synopsis

`lag config partner port <portlist> [port]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`port` is an integer between 1 and 26 specifying partner’s port number.

Description

Assigns the administrative value of the port number for the protocol partner. For example, to specify that local port 3 is connected to protocol partner’s port 5, execute the following command:

```
# lag config partner port 3 5
```

When the LACPDUs are exchanged between the actor (the local switch) and the protocol partner, the locally assigned partner’s port number will be replaced with a real partner’s port number communicated inside the LACPDU. By factory default, local port 1 is assigned partner’s port 1, local port 2 is assigned partner’s port 2, etc. If optional arguments are not specified, display partner's ports for all the specified switch ports.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Assign Partner State

Synopsis

`lag config partner state <portlist> [state]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`state` is an 8-bit value in hexadecimal notation describing the state of the partner aggregator state machines. The first most significant bit describes the Actor_State (LACP_Activity), the second most significant bit describes LACP_Timeout, the third bit corresponds to Aggregation, the fourth bit corresponds to Synchronization, the fifth bit corresponds to Collecting, the sixth bit corresponds to Distributing, the seventh bit corresponds to Defaulted, and the eighth bit corresponds to Expired. If no optional argument is specified, display current settings for all specified ports.

Description

This command administratively sets the actor state. Remember that when the actor (the local switch) and the partner exchange LACPDUs, the actor’s state will reflect the actual state communicated by the protocol partner. This command displays administrative values of Actor_State for the protocol partner assigned to all specified ports.

Display or Set Link Decision Method

Synopsis

`lag config cost [method]`

where

`method` is one of the following keywords: ft or maxspeed.

Description

Set the method Spanning Tree will use to calculate the path cost. STP calculates the path cost based on the speed of the link. Refer to the IEEE 802.1D Table 8-5 for the definitions of the Path Cost parameter values in relation to the link speed. The port path cost may change as a result of a change in the port aggregation. Two different algorithms are employed in calculating the aggregated link path cost. The first one favors the maximum speed (“maxspeed”). This algorithm always assigns a better path cost to the higher speed link. The second algorithm favors the link resiliency and assigns a better path cost to the aggregated links (“ft”). The “lag config cost [method]” command allows the user to select one of the two algorithms. By default, the algorithm that favors maximum speed will be used. If the user selects the algorithm that

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

favors resiliency, then seven or more aggregated links will have a better path cost than the next higher link speed. For example, if the “ft” method is selected, then an aggregation of seven 100 Mbs links will have a better path cost than a single 1000 Mbs link. On the other hand, when a “maxspeed” method is selected, then a 1000 Mbs link will always have a better path cost than an aggregation of 100 Mbs links.

Configure Static NoTimeout

Synopsis

`lag config static notimeout <portlist> [enable]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable Link Aggregation timeout on a port. Setting a port to “notimeout ON” affects it such that once a link aggregation is formed using a regular LACPDUs exchange mechanism, the port will stay in the aggregation even if it stops receiving LACPDUs from its link partner. In other words, a port set to be “static notimeout ON” will no longer timeout its Link Aggregation settings once the aggregation is formed. Setting a port to “static notimeout OFF” restores its regular LAG operation. By default, all ports are set to “static notimeout OFF”.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Churn Detection State Machine Information

Synopsis

`lag show churn`

Description

Displays Actor and Partner Churn Detection State Machine information. The Churn Detection machines detect the situation where a port is operable, but the Actor and Partner have not attached the link to an Aggregator and brought the link into operation within a specified time period. This command displays a table similar to the following:

```
************************************************************************
                    Churn State Machines and Debug Info
------------------------------------------------------------------------
P#  Astate       a_churn  Acount  Pstate       p_churn  Pcount  enabled/link
------------------------------------------------------------------------
01  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
02  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
03  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
04  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
05  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
06  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
07  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
08  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
09  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
10  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
11  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
12  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
13  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
14  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
15  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
16  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
17  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
18  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
19  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
20  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
21  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
22  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
23  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
24  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
25  A_CHURN_MON  NO       000000  P_CHURN_MON  NO       000000  NO  /0
26  NO_A_CHURN   NO       000000  NO_P_CHURN   NO       000000  YES /1
```

P# is a port number

`Astate` shows the state of the Actor Churn Detection state machine, which can be one of the following: NO_A_CHURN (NO ACTOR CHURN), A_CHURN_MON (ACTOR CHURN MONITOR), A_CHURN (ACTOR CHURN).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

`a_churn` is a port variable set to either True (YES) or False (NO). This variable indicates that the Actor Churn Detection machine has detected that a local port configuration has failed to converge within a specified time, and that management intervention is required.

`Acount (Actor Count)`
shows how many times Actor Churn Detection machine entered the ACTOR_CHURN state.

`Pstate` shows the state of the Partner Churn Detection state machine, which can be one of the following: NO_P_CHURN (NO PARTNER CHURN), P_CHURN_MON (PARTNER CHURN MONITOR), P_CHURN (PARTNER CHURN).

`p_churn` is a port variable set to either True (YES) or False (NO). This variable indicates that the Partner Churn Detection machine has detected that a remote port configuration has failed to converge within a specified time, and that management intervention is required.

`Pcount (Partner Count)`
shows how many times Partner Churn Detection machine entered the PARTNER_CHURN state.

`enabled/link` shows the state of the port_enabled variable and the state of the link. They both should match. The port_enabled variable can be set to either True (YES) or False (NO). When set to True, it indicates that the link has been established and the port is operable. The link is displayed as a numerical value 0 (Down) or 1 (Up).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Log Management

Write a Message to the Log

Synopsis

`log message [message]`

where

`message` is an ASCII String.

Description

Write a message to the log. If no message is provided, output date and time stamp.

Enable or Disable Console Logging

Synopsis

`log console [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable console (serial port) logging on the CPC441x. Logging stores the commands and messages from that time when enabled forward. If no argument is provided, display the current configuration.

Enable or Disable Logging to a File

Synopsis

`log file set [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable logging to a file on the CPC441x. If no argument is provided, display the current configuration.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set the Log File Name

Synopsis

`log file name [filename]`

where

`filename` is an ASCII Label.

Description

Set the file name of the log file. If no argument is provided, display the current configuration.

Enable or Disable Remote Logging to an IP Address

Synopsis

`log remote set [index] [enable]`

where

`index` is an integer type between 1 and 5 (inclusive).

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable logging to a remote machine (running `syslogd`). If no arguments are provided, a list of addresses and current the current state (logging enabled/disabled) is displayed. If an index is provided, only the information for that particular index is displayed.

Set the IP Address of Remote Logging

Synopsis

`log remote ip [index] [ip_addr]`

where

`index` is an integer type between 1 and 5 (inclusive).

`ip_addr` is an IP Address (see “IP Address” on page 74.)

Description

Set the IP address of remote logging servers. If no arguments are provided, a list of addresses and their current states are provided.

If an index is given, only the information for that particular index is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Note: *To use remote logging, the host machine must be running* `syslogd` *with remote logging enabled (start the server with the "-r" option). Log messages are sent to the server with a facility of DAEMON (24), and a priority of NOTICE (5).*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Network Diagnostics

Enable or Disable CPU Mirror Mode

Synopsis

`mirror cpu [port]`

where

`port` is a Port number, or none (see “Port” on page 74.)

Description

Setting this variable to a port number causes packets sent by the CPU to be sent also to the specified port. Setting the port number to `zero` or `none` disables this feature. This setting is independent of the `mirror mode` and `mirror to` settings. If no argument is specified, the current setting is displayed.

Set Mirror Mode

Synopsis

`mirror mode [mode]`

where

`mode` is an optional argument specifying the desired state of the port mirroring function. It is specified on the command line with the keywords: `l2`, `l3`, `off`. The cpu mirroring function is not affected by this setting. Use “mirror cpu” to control cpu mirroring.

Description

This command enables or disables port mirroring on the switch. If no arguments are specified, the “mirror mode” command displays the current mode settings. To use port mirroring, a “mirror” and “mirror-to” port need to be specified with the “mirror to” and “mirror ingress/egress” commands.

The optional keywords select the following functions:

`l2` enable port mirroring of packets that are Layer2 switched.

`l3` enable port mirroring of packets that are Layer3 switched.

`off` disable mirroring from this port.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Mirror To Port

Synopsis

`mirror to [port]`

where

`port` is a Port number (see “Port” on page 74.)

Description

This command allows the user to set the “mirror-to” destination port. If no arguments are set, then the current destination port is displayed. To use port mirroring, it must be globally enabled using the “mirror mode” command, and the source port must be specified with the “mirror ingress/egress” command.

Set Ingress Port(s) to be Mirrored

Synopsis

`mirror ingress <portlist> [mode]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`mode` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable mirroring of frames coming from a specified set of ports. If mode is not specified, then the current “ingress” status on the specified ports is displayed.

Set Egress Port(s) to be Mirrored

Synopsis

`mirror egress <portlist> [mode]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`mode` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable mirroring of frames being transmitted out the specified ports. If *`mode`* is not specified, then the current “egress” status on the specified ports is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Ping

Synopsis

`ping <host> [n]`

where

`host`	is the name or IP address of the target host.
`n`	is a decimal integer specifying the number of times to attempt the ping.

Description

Use ping to test for host accessibility. Defaults to a single ping if *n* is not specified. The command will send pings continuously if *n* is 0.

Trace Route

Synopsis

`traceroute <host> [interface]`

where

`host`	is the name or IP address of the target host.
`interface`	is an Interface Description keyword (See “Interface Description” on page 74.)

Description

Use traceroute to determine the path taken to reach a host.

Note: *Traceroute can only be run from one user interface at a time, either CLI or Telnet.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Online Integrity Test Configuration

Enable, Disable or Display All Level One Online Integrity Tests

Synopsis

`integrity levelone [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable all level one online integrity tests. If no argument is given the current value is displayed.

Enable, Disable or Display All Level Two Online Integrity Tests

Synopsis

`integrity leveltwo [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable all level one online integrity tests. If no argument is given the current value is displayed. Level two integrity tests validate the correct operation of key switching tasks such as Spanning Tree, Address Learning, etc. (See“Diagnostic Tools” on page 445.)

Enable, Disable, or Display an Online Integrity Test

Synopsis

`integrity enable <testname> [enable]`

where

`testname` is a string.

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable a single online integrity test. If no argument is given the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display the Current Online Integrity Test Settings

Synopsis

`integrity show`

Description

Display all online integrity tests with their current settings.

Display or Set an Action for an Online Integrity Test

Synopsis

`integrity action <testname> <action> [enable]`

where

`testname` is a string.

`action` is one of the following: ignore, log, reboot, sendtrap, halt, offline.

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable an online integrity test action. If no argument is given the current value is displayed.

Display or Set Level One Integrity Timer Value

Synopsis

`integrity levelonetimer [value]`

where

`value` is the value the user wants to configure.

Description

Display or set the time interval between the running of the level one integrity test suite. The units are in deciseconds. The minimum value is 1 (1/10 of 1 second). The maximum value is 3000 (thirty seconds).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Password Management

The factory default password is `password`. If the configured password is lost or forgotten, contact Performance Technologies for a remedy.

Email: support@pt.com

Tel: 585-256-0200

Fax: 585-256-0791

Set the System Password

Synopsis

`password`

Description

This command sets the password for the system (board level). This password is required to gain access to the CPC441x through the CLI or Web Interface. The password command prompts the user for the existing password and then prompts for the new password twice. The existing password must match the current setting and both entries of the new password must be the same. The user input is not displayed; asterisks (**) are displayed for the characters entered by the user. Valid passwords may be up to16 printable ASCII characters.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Port Commands

Give a Symbolic Name to a Port

Synopsis

`port name <port> [name]`

where

`port` is the Port number (see “Port” on page 74.)

`name` is an ASCII Label of up to 16 printable characters.

Description

Assign a symbolic name to a port. The symbolic name will be shown in place of the port number in status displays. If no argument is provided, display the current setting.

Configure a Port

Synopsis

`port config <portlist> [autoneg] | <[speed] [duplex] [flow]>`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`autoneg` is an argument specifying the desired autonegotiation state. The keyword `auto` sets the port to autonegotiation. The keyword `off` sets the port to manual configuration. If the keyword *`off`* is entered, then *`speed`*, *`duplex`*, and *`flow`* arguments are required.

When autonegotiate is enabled, the following port signals and characteristics are sensed and corrected (if needed) to match the connected device.

TX+ and TX- Polarity

RX+ and RX- Polarity

TX and RX cross-connect

Full or Half Duplex

10 or 100 Mbps speed

`speed` is an optional argument specifying the desired speed. It is specified on the command line with the keywords *`auto`*, *`10`*, *`100`*, *`1000`*.

`duplex` is an optional argument specifying the desired duplex setting. It is specified on the command line with the keyword *`full`* or *`half`*.

`flow` is an optional argument specifying the desired flow control setting. It is a Boolean argument (see “Boolean” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Configure a set of ports. The arguments include: a list of ports to configure, and the configuration. If the configuration is autonegotiate, then `autoneg` is the only required parameter. Otherwise, the speed, duplex and flow control values must be specified. If no configuration argument is provided, display the current setting.

When autonegotiate is enabled, the port polarity sense and MDX are also enabled.

Set Link for a Port (Enable or Disable)

Synopsis

`port link <portlist> [mode]`

where

`portlist`	is a List of Port numbers (see "List" and "Port" on page 74.)
`mode`	is either the keyword `up` or `down`. The keyword `up` indicates the port is enabled and `down` indicates the port is disabled.

Description

Set the link on the ports specified to up (enabled) or down (disabled). If no mode is given, display the current configuration for the specified ports.

Configure Autonegotiation Advertisement Parameters

Synopsis

`port autoneg admin advertise <portlist> [A10MB_HD] [A10MB_FD] [A100MB_HD] [A100MB_FD] [A1000MB_HD] [A1000MB_FD] [asym] [sym] [bothAandS]`

where

`portlist`	is a List of Port numbers (see "List" and "Port" on page 74.)
`A10MB_HD`	is an optional argument specifying whether to advertise 10M Half Duplex. It is a Boolean argument (see "Boolean" on page 74.)
`A10MB_FD`	is an optional argument specifying whether to advertise 10M Full Duplex. It is a Boolean argument (see "Boolean" on page 74.)
`A100MB_HD`	is an optional argument specifying whether to advertise 100M Half Duplex. It is a Boolean argument (see "Boolean" on page 74.)
`A100MB_FD`	is an optional argument specifying whether to advertise 100M Full Duplex. It is a Boolean argument (see "Boolean" on page 74.)
`A1000MB_HD`	is an optional argument specifying whether to advertise 1000M Half Duplex. It a Boolean argument (see "Boolean" on page 74.)
`A1000MB_FD`	is an optional argument specifying whether to advertise 1000M Full Duplex. It a Boolean argument (see "Boolean" on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

asym	is an optional argument specifying whether to advertise Asymmetric Pause (from partner). It is a Boolean argument (see “Boolean” on page 74.)
sym	is an optional argument specifying whether to advertise Symmetric Pause (to and from partner). It is a Boolean argument (see “Boolean” on page 74.)
bothAandS	is an optional argument specifying whether to advertise both Asymmetric and Symmetric Pause. It is a Boolean argument (see “Boolean” on page 74.)

Description

Set the autonegotiation advertisement values for ports. The values determine what the port will offer during autonegiation to its link partner. If none of the optional settings are provided, the current setting will be displayed. If the user enters a subset of the optional settings, then only those settings provided will be modified, the rest will remain unchanged.

Example 1: Display current setting for port 1

```
# port autoneg admin advertise 1

        Port Autonegotiation Advertisement Settings

  Port   10HD   10FD   100HD  100FD  Asym   Sym    BothAandS  1000HD   1000FD

-------------------------------------------------------------------------------
  1      *      *      *      *      -      *      -          -        *
-------------------------------------------------------------------------------


*   : Mode is advertised
-   : Mode is not advertised
```

Example 2: Set all values in advertisement

```
# port autoneg admin advertise 1 on on on on off on off off on
```

Example 3: Modify selected values to advertise (e.g., 100M Half Duplex Off)

See “Entering Commands” on page 75 for a description of setting selected optional arguments.

```
# port autoneg admin advertise 1 A100MB_HD=off
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Restart Autonegotiation

Synopsis

`port autoneg admin restart <portlist>`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Restart the autonegotiation process for specified port(s). If autonegotiation signaling is disabled (see ‘port config’), then this command has no effect.

Display Statistics for a Port

Synopsis

`port stats <port>`

where

`port` is the Port number (see “Port” on page 74.)

Description

Display the configuration, RMON Statistics and MAC Address for the specified port.

Configure Port Frame Size

This command allows the user to take advantage of the Layer2 support for Jumbo Frames in the switch. The maximum frame size can be set per port, allowing larger than standard frames to be received on the port.

This control only manages whether large frames will be allowed into the switch. It does not control transmission of these frames. Large frames may be sent to any port in the VLAN of a receiving port that has large frames enabled.

Synopsis

`port framesize <portlist> [value]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`value` is an integer describing the frame size desired. This value should be on a 32-bit boundary.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Specify the frame size per port. If no value is given, display the current setting. Support for Jumbo Frames allows larger than standard frames to be received on a port. This command controls receiving large frames; it does not affect transmission of these frames. Large frames may be sent to any port in the VLAN of a receiving port that has large frames enabled.

Note: *Ethernet CRC-32 loses its effectiveness above approximately 12000 bytes.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Routing Management

The CLI commands for routing management are divided into separate sections for RIP (Routing Information Protocol), below, and “OSPF (Open Shortest Path First) Management” on page 189.

RIP (Routing Information Protocol) Management

Enable or Disable RIP

Synopsis

`route rip [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the RIP routing. If “enable” is not specified, the current value is displayed.

Set RIP Configuration

Synopsis

`route rip set <ip> [authtype] [authkey] [sendtype] [receivetype] [defaultmetric]`

where

`ip_addr` is an IP Address (see “IP Address” on page 74.)

`authtype` is one of the following:

`noAuthentication`

`simplePassword`

`md5`

The default is *`noAuthentication`*.

`authkey` is a 16 byte key used as a clear text password or md5 key.

`sendtype` is one of the following:

`doNotSend`

`ripVersion1`

`rip1Compatible`

`ripVersion2`

`ripV1Demand`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

ripV2Demand.

The default is *rip1Compatible*.

receivetype is one of the following:

doNotReceive

rip1

rip2

rip1OrRip2.

The default is *rip1OrRip2*.

defaultmetric
is an integer used to represent the hop count. The range is 0 to 15. The default is 0.

Description

This command will set the specified values on the interface associated with the specified IP address.

Advertise Static Routes

Synopsis

route rip advertise static [enable]

where

enable is a Boolean type (See “Boolean” on page 74.)

Description

Informs RIP whether to advertise any static routes configured on the switch. Use this command to enable advertising before adding any static routes.

Advertise Default Route

Synopsis

route rip advertise default [enable]

where

enable is a Boolean type (See “Boolean” on page 74.)

Description

Informs RIP whether to advertise a default route. Use this command to enable advertising before adding a default route.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Advertise OSPF Routes

Synopsis

`route rip advertise ospf [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Informs RIP whether to advertise OSPF routes. Use this command to enable advertising before enabling OSPF.

Enable or Disable Border Gateway Filtering

Synopsis

`route rip advertise border [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enables or disables border gateway filtering. RIP will ignore the restrictions necessary for RIPv2 to interoperate with RIPv1. This should be disabled only if no RIPv1 routers are present in the network. See RFC1723 section 3.3 and RFC1058 section 3.2 for more information.

Display per Port RIP Statistics

Synopsis

`route rip stats`

Description

This command will display all appropriate statistics on all interfaces. The display will indicate Bad Packets Received, Bad Routes Received, and Updates Sent.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Disable RIP on a Particular Interface

Synopsis

`route rip disable <ip>`

where

`ip_addr` is an IP Address (see “IP Address” on page 74.)

Description

This command will disable RIP on the specified interface.

Display RIP Configuration

Synopsis

`route rip show`

Description

This command will show the current RIP configuration for each interface.

OSPF (Open Shortest Path First) Management

Enable or Disable OSPF

Synopsis

`route ospf [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the OSPF routing protocol for this device. If “enable” is not specified, the current value is displayed. When enabling OSPF, insure the ‘route ospf id’ (“Set Router ID” on page 190) is set to a valid interface.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Autonomous System Border Router

Synopsis

`route ospf asborder <enable>`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

This command specifies whether this router is configured as an Autonomous System border router. If “enable” is not specified, the current value is displayed.

Set Router ID

Synopsis

`route ospf id [id]`

where

`ip_addr` is an IP Address (see “IP Address” on page 74.)

Description

Configure the router ID for the current switch. If no ID is specified, the current value is displayed. If router ID is not set, then OSPF selects the lowest numerical-value IP address of the sw network interfaces as its router ID.

Note: *The ‘route ospf enable’ must be off before setting this id.*

Enable or Disable Opaque LSAs

Synopsis

`route ospf opaque <enable>`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable opaque LSAs (LSA type 9, 10 and 11). By default, opaque LSAs are disabled. This setting must match the setting of other routers on the network (note that Cisco routers enable opaque LSAs by default).

The following command will enable opaque LSAs:

```
route ospf opaque on
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Stub Area and Metric

Synopsis

`route ospf stub add <area> [tos] [metric]`

where

`area`	is a 32-bit integer in dotted decimal notation. The allowed range is 0.0.0.0 to 255.255.255.255.
`tos`	is an integer.
`metric`	is a32-bit decimal value. If the area has been configured as a stub area, and the router itself is an area border router, then `metric` indicates the cost of the default summary link that the routers should advertise into the area. The range is 1-65535.

Description

This command makes the specified area a stub area. A stub area prevents ASBR LSAs (Type 5) and ASBR summary LSAs (Type 4) from flooding the routers contained within the area. This command allows the user to assign a metric. If no metric is specified, then OSPF uses a formula (100000000 / ifSpeed) to calculate the default metric. Before an area can be configured as a stub area it must first be created using the `route ospf area` command.

Remove a Stub Area

Synopsis

`route ospf stub remove <area> [tos]`

where

`area`	is a 32-bit integer in dotted decimal notation. The allowed range is 0.0.0.0 to 255.255.255.255.
`tos`	is an integer.

Description

Delete the entry specified by “area” and “tos.” If no value for “tos” is provided, this will be set to zero.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display All Stub Areas

Synopsis

`route ospf stub show`

Description

Display the stub area table.

Add New Stub Area

Synopsis

`route ospf area add <area> [as] [summary]`

where

`area` is a 32-bit integer in dotted decimal notation. The allowed range is 0.0.0.0 to 255.255.255.255.

`as` (area summaries) is one of the following strings or its corresponding number, defining external routing capabilities:

importExternal (1) the area allows external LSAs (type 4 and type 5). This is the default value.

importNoExternal (2) the area is configured to be a stub area (a stub area excludes external advertisements, i.e., LSAs type 4 and type 5). A backbone area (area 0.0.0.0) cannot be configured as a stub area. Also, virtual links cannot be configured through a stub area.

importNSSA (3) allows importing Not So Stubby Area (NSSA) LSAs, type 7.

`summary` is one of the following strings or its corresponding number:

noAreaSummary (1) the router will neither originate nor propagate summary LSAs into the stub area.

sendAreaSummary (2) the router will summarize and propagate LSAs.

Description

Add a new area and specify whether this area will allow or exclude external advertisements and/or NSSA LSAs. If “as” is not specified, the default is “importExternal,” meaning the new area will allow type 4 and type 5 LSAs. If set to exclude LSAs, the new area is a stub area.

For example, the following command will create area 2 as a regular area that allows external LSAs:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
# route ospf area add 0.0.0.2
```

The following command will create area 0.0.0.3 and configure it to be a stub area:

```
# route ospf area add 0.0.0.3 importNoExternal
```

Remove an OSPF Area

Synopsis

`route ospf area remove <area>`

where

`area` is a 32-bit integer in dotted decimal notation. The allowed range is 0.0.0.0 to 255.255.255.255.

Description

Delete the specified area from the area table.

Display OSPF Areas

Synopsis

`route ospf area show`

Description

Display a list of all configured areas.

Configure an OSPF Interface

Synopsis

`route ospf interface admin <interface_ip> [admin]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`admin` is a Boolean, either `on` or `off`. If the interface is administratively configured to be “on,” then it will be advertised in OSPF Link State Advertisements; if “off,” this interface will be excluded from the LSA advertisements.

Description

Includes or excludes the specified links from the route advertisements. If `admin` is not specified, the current value is displayed.

Example:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Three interfaces (sw1 - sw3) are configured as subnetworks, 172.16.1.0, 172.16.2.0 and 172.16.3.0, respectively. The following command will exclude sw1 from participating in the OSPF advertised routes:

```
# route ospf interface admin 10.10.1.1 off
```

The switch will advertise only 172.16.2.0 and 172.16.3.0 and will not advertise 172.16.1.0.

Specify an Interface to be Advertised and Associate It with an Area

Synopsis

`route ospf interface add <interface_ip> [area]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`area` is a 32-bit integer in dotted decimal notation. The allowed range is 0.0.0.0 to 255.255.255.255.

Description

Associate an area with the specified interface. If “area” is not specified, the current value is displayed. This is one of the most basic commands. It tells the OSPF process what interface to advertise out. Because IP Multihoming allows the user to configure multiple IP addresses on a single interface, this command specifies a particular IP address which belongs to an interface to be advertised by the OSPF process.

For example, the following command informs the OSPF process to assign a network interface with an IP address 10.10.1.1 to area 0, and advertise it to the OSPF network:

```
# route ospf interface add 10.10.1.1 0.0.0.0
```

Remove an Interface from OSPF

Synopsis

`route ospf interface remove <interface_ip>`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

Description

Remove an interface address from the OSPF process. This command allows the user to delete the specified IP address from the OSPF area. The deleted interface’s IP address will no longer be advertised by the OSPF process.

For example the following command informs the OSPF process that the IP address 10.10.1.1 will no longer belong to any area and will no longer be advertised by the OSPF process:

```
# route ospf interface del 10.10.1.1
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set OSPF Authentication Key

Synopsis

`route ospf interface authkey <interface_ip> <authkey>`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`authkey` is an ASCII label

Description

Configure the authentication key for the specified interface IP address.

Note: *This value is write only, and cannot be read.*

Set OSPF Authentication Type

Synopsis

`route ospf interface authtype <interface_ip> [authtype]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`authkey` is one of the following ASCII labels: *`none`* or *`simplePassword`*

Description

Configure the authentication type to be used for the specified interface IP address.

Set OSPF Dead Interval

Synopsis

`route ospf interface dead <interface_ip> [dead]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`dead` is a decimal integer value that specifies the number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Configure the OSPF dead interval for the specified interface IP address. The dead interval is the number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down. This should be some multiple of the Hello interval, and it must be the same for all routers attached to a common network. The default is 40. Be sure not to set this interval too large or too small: if it is too large, a dead router will go undetected. If it's smaller than the Hello interval, it will never form an adjacency.

Set OSPF Transit Delay

Synopsis

`route ospf interface delay <interface_ip> [delay]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`delay` is a decimal integer value which specifies the number of seconds it takes to transmit a link state update packet over this interface.

Description

Configure the OSPF Transit delay for the specified interface IP address. The transit delay is the estimated number of seconds it takes to transmit a link state update packet over this interface. The default is 1. Although the range is 1 - 32-bit integer, use a realistic value which truly reflects your link's capability. If `delay` is not specified, the current value is displayed.

Set OSPF Hello Interval

Synopsis

`route ospf interface hello <interface_ip> [hello]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`hello` is a decimal integer value which specifies the length of time, in seconds, between the Hello packets that the router sends on the interface.

Description

Configure the OSPF Hello interval for the specified interface. The hello interval is the length of time, in seconds, between the hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network. The default is 10 seconds. Although the range is 1 - 32 bit decimal, use moderation when changing this value. If `hello` is not specified, the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set OSPF Interface Priority

Synopsis

`route ospf interface priority <interface_ip> [priority]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

`priority` is an integer value specifying the priority of this interface. The range is 0 - 255, and the default is 1.

Description

Configure the OSPF interface priority. Used in multi-access networks, this field is used in the designated router election algorithm. A value of 0 signifies that that router is not eligible to become the designated router on this particular network. In the event of a tie in this value, routers will use their Router ID as a tie breaker. If `priority` is not specified, the current value is displayed.

Display OSPF Interface Table

Synopsis

`route ospf interface show [interface_ip]`

where

`interface_ip` is an interface IP address (e.g., 10.10.1.1)

Description

Show the OSPF interface table. If an interface IP address is specified, greater detail is provided for that interface.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

For example:

```
# route ospf interface show

Iface   IP          Area      State                     Admin State
-------------------------------------------------------------------
sw1     10.10.1.1   0.0.0.0   backupDesignatedRouter    on
sw2     20.20.1.1   0.0.0.0   designatedRouter          on
sw3     30.30.1.1   0.0.0.0   designatedRouter          on

# route ospf interface show 10.10.1.1

               Interface: sw1
                      IP: 10.10.1.1
                    Area: 0.0.0.0
          Interface Type: broadcast
            Admin Status: on
                Priority: 1
                   Delay: 2
     Retransmit Interval: 5
          Hello Interval: 10
       Router Dead Time: 40
           Poll Interval: 120
                   State: backupDesignatedRouter
       Designated Router: 10.10.1.2
Backup Designated Router: 10.10.1.1
                  Events: 3
               Auth Type: none
```

Enable or Disable Default Route Redistribution

Synopsis

`route ospf redistribute default <enable>`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

If enabled, the OSPF will install and redistribute external LSAs with the default route 0.0.0.0 as the forwarding address. By default, default route redistribution is disabled.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Enable or Disable Static Route Redistribution

Synopsis

`route ospf redistribute static <enable>`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

If enabled, OSPF will redistribute statically configured gateways to its peers. By default, redistribution of static routes is disabled.

Enable or Disable RIP Route Redistribution

Synopsis

`route ospf redistribute rip <enable>`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

If enabled, OSPF will redistribute RIP routes to its peers. By default, RIP redistribution is disabled.

Display OSPF General Settings

Synopsis

`route ospf show general`

Description

Display OSPF general information, including:

`Router ID` the highest IP address of the active interface on the router.

`Admin Status` the administrative status of OSPF in the router. The value “enabled” indicates that the OSPF process is active on at least one network interface, “disabled” disables it on all interfaces.

`Version` the current version number of the OSPF protocol is 2.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

`AS Border Router`
: a flag that indicates whether the OSPF router is configured as an Autonomous System Border Router (ASBR).

`External LSA Count`
: the number of external LSA (type 5) advertisements in the Link State Database.

`External LSA Checksum Sum`
: a sum of the LSA checksums of the external link-state advertisements contained in the link-state database.

`TOS Support` the router support for Type-of-Service routing (true/false)

`New LSA received`
: the number of link-state advertisements received.

`External LSDB Limit`
: the maximum number of non-default AS-external-LSA entries that can be stored in the link-state database. If the value is -1, then there is no limit.

`Multicast Extensions`
: a Bit Mask indicating whether the router is forwarding IP multicast (Class D) datagrams based on the algorithms defined in the Multicast Extensions to OSPF.

`Exit Overflow Interval`
: the number of seconds after entering OverflowState that the CPC441x will attempt to leave OverflowState.

`Demand Extension Support`
: the router support for demand routing.

Display Link State Database

Synopsis

`route ospf show database`

Description

Display contents of the link-state database. The database is divided into sections, reflecting the information processed from different types of LSAs, and it shows from which router the LSA was received:

`Router Link States` is listing of routers contained in Type 1 LSAs per each area.

`Net Link States` contain the LSAs received on a multi-access network (Type 2 LSAs).

`Summary Net Link States`
: are the summary links injected by the Autonomous Border Routers (ABRs) and are propagated using Type 3 LSAs.

`Summary ASB Link States`
: contain links from Type 4 LSAs and AS External Link States from Type 5.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The output of the `route ospf show database` command appears below:

```
                    Router Link Status
Area     Link ID       Router ID     Age   Sequence     Chksum
-------------------------------------------------------------------
0.0.0.0  172.16.20.10  172.16.20.10  1060  0x800000076  0x46BA
0.0.0.0  172.16.20.20  172.16.20.20  890   0x800000020  0x4568

                    Net Link States
Area     Link ID       Router ID     Age   Sequence     Chksum
-------------------------------------------------------------------
0.0.0.0  172.16.10.10  172.16.20.10  1061  0x800000073  0x4BBA
0.0.0.0  172.16.10.20  172.16.20.20  840   0x800000044  0x4599

                  Summary Net Link States
Area     Link ID       Router ID     Age   Sequence     Chksum
-------------------------------------------------------------------
0.0.0.0  10.20.0.0     172.16.20.10  69    0x800000063  0x486A
0.0.0.0  10.1.0.0      172.16.20.40  840   0x800000014  0x4119

                    Summary ASB Link States
Area     Link ID       Router ID     Age   Sequence     Chksum
-------------------------------------------------------------------
0.0.0.0  172.1.50.11   172.16.20.50  88    0x800000066  0x5678
0.0.0.0  172.1.50.55   172.16.20.60  96    0x800000023  0x3411
```

Display OSPF Neighbors

Synopsis

`route ospf show neighbor`

Description

Display all the known OSPF neighbors. Below is an example of a Show Neighbor display:

```
IP Address   Router ID     OptnsPri  State  Evnt  Dynamic
-------------------------------------------------------------------
172.16.1.1   172.16.1.12   1         full   866   on
172.16.30.3  172.16.30.32  1         full   874   on
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Create a Virtual Connection

Synopsis

`route ospf virtual add <area> <neighbor>`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.

Description

Add a new entry to the virtual interface table. The area is specified by `area` and the neighbor by `neighbor`. This command is for the non-broadcast network. The CPC441x is an Ethernet switch, and therefore it is not necessary to execute the neighbor command in order for the neighbor relationships to be formed

Set Authentication Key for a Virtual Connection

Synopsis

`route ospf virtual authkey <area> <neighbor> <authkey>`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.
`authkey`	is an ASCII label.

Description

Configure the authentication key for the specified area and neighbor.

Note: *This value is write only, and cannot be read.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Authentication Type for a Virtual Connection

Synopsis

`route ospf virtual authtype <area> <neighbor> [authtype]`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.
`authtype`	is an ASCII string which can be one of the following: *`none`* *`SimplePassword`*

Description

Configure the authentication type to be used for the specified area and neighbor. `none` indicates that no authentication is specified. `simplePassword` specifies simple password authentication string type. If `authtype` is not specified, the current value is displayed.

Set Dead Interval for a Virtual Connection

Synopsis

`route ospf virtual dead <area> <neighbor> [dead]`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.
`dead`	is a decimal integer value that specifies the number of seconds a router's Hello packets have not been seen before its neighbors declare the router down.

Description

Configure the dead interval for the specified area and neighbor. The dead interval is the number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down. This should be some multiple of the Hello interval, and it must be the same for the virtual neighbor. The default is 40. Be sure not to set this interval too large or too small: if it's too large, a dead neighbor will go undetected. If it's smaller than the Hello interval, it will never form an adjacency. If `dead` is not specified, the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Transit Delay for a Virtual Connection

Synopsis

`route ospf virtual delay <area> <neighbor> [delay]`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.
`delay`	is a decimal integer value that specifies the number of seconds required to transmit a link state update packet over this interface.

Description

Configure the transit delay for the specified area and neighbor. The transit delay is the estimated number of seconds it takes to transmit a link-state update packet over this interface. The default is 1. The range is 1 - 32 bit integer, but use a realistic value that reflects your link's capabilities. If `delay` is not specified, the current value is displayed.

Remove a Virtual Connection

Synopsis

`route ospf virtual remove <area> <neighbor>`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.

Description

Delete the entry specified by `area` and `neighbor` from the virtual interface table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Hello Interval for Virtual Connection

Synopsis

`route ospf virtual hello <area> <neighbor> [hello]`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.
`hello`	is a decimal integer value which specifies the length of time, in seconds, between the Hello packets that the router sends on the interface.

Description

Configure the Hello interval for the specified area and neighbor. The Hello interval is the length of time, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for the virtual neighbor.The default is 10 seconds. Although the range is 1 - 32 bit decimal, use moderation when changing this value. If `hello` is not specified, the current value is displayed.

Set Retransmit Interval for a Virtual Connection

Synopsis

`route ospf virtual retrans <area> <neighbor> [retransmit]`

where

`area`	is a 32-bit integer specified in a dotted decimal notation. The allowed range is 0.0.0.0 - 255.255.255.255.
`neighbor`	is an IP address of the neighbor router.
`retransmit`	is decimal integer specifying the number of seconds between link-state advertisement retransmissions.

Description

Configure the retransmit interval for the specified area and neighbor. The retransmit interval is the number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. The default value is 5 and the range is 1-255. This value is also used when retransmitting database description and link-state request packets. This value should be well over the expected round-trip time. If `retransmit` is not specified, the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Virtual Connections

Synopsis

`route ospf virtual show`

Description

Display the entries in the virtual interface table.

Add a Static Route

Synopsis

`route add <destination> <netmask> <nexthop> [description] [usehw]`

where

`destination` is an IP address, or the keyword `default`

`netmask` is an IP address.

`nexthop` is an IP address (see “IP Address” on page 74.)

`description` is an ASCII String

`usehw` is a Boolean type (see “Boolean” on page 74.)

Description

Add a route to the routing table. `Destination` is the static route host or subnet IP destination address, or the keyword `default`. `Netmask` is the mask for this IP destination. `Nexthop` is the IP address of the next hop of this route. (In the case of a route bound to an interface that is realized via a broadcast media, the value of this field is the agent’s IP address on that interface.) If `usehw` is set, the hardware routing will be used for this entry.

Delete a Static Route

Synopsis

`route delete <destination>`

where

`destination` is an IP address, or `default`.

Description

Delete the entry specified by `destination` or the default route if `default` is specified.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display the Static Routes

Synopsis

```
route show
```

Description

Display the current routing table for the switch.

Display the Complete Routing Table

Synopsis

```
route dump
```

Description

Display the entire routing table (static and dynamic entries) currently configured on the switch.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Shell Commands

Echo a Message

Synopsis

`echo [message]`

where

`message` is an ASCII printable string of characters terminated by a carriage return `<cr>`.

Description

Display the message on the standard output.

Execute a Script File

Synopsis

`exec <file_name>`

where

`file_name` is the name of a script file containing Lua or CLI commands.

Description

Execute a CLI script file or Lua program. If the file has a `.lua` extension, then the file executed by the Lua interpreter, otherwise it is processed by the CLI.

Suspend Execution

Synopsis

`sleep <time>`

where

`time` is a decimal integer representing seconds.

Description

Suspend execution (shell or script) for the specified time.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Command Line Help

Synopsis

`help [command]`

where

`command` is any existing command name.

Description

Display help for the specified command or display the list of available commands.

Exit Out of Performance Technologies CLI

Synopsis

`exit`

Description

Exit (logout) of the current Performance Technologies CLI session.

Display or Set Octet String MIB Object

Synopsis

`idbstring <object> [index] [value]`

where

`object` is an ASCII Label.

`index` is a decimal integer.

`value` is an ASCII String.

Description

Display or set the `index` instance of the MIB string specified by `object`. If index is not specified, 0 will be used. To set a string object, specify a value. For example, to set the first instance of the user definable string cpc4400:cpc4400UsrVarString to the value *test*, enter the following:

```
# idbstring cpc4400:cpc4400UsrVarString 0 test
```

To display this value, enter the following:

```
# idbstring cpc4400:cpc4400UsrVarString 0
```

This will yield: `test`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set Integer MIB Object

Synopsis

`idbu32 <object> [index] [value]`

where

`object`	is an ASCII Label.
`index`	is a decimal integer.
`value`	is a decimal integer.

Description

Display or set the `index` instance of the MIB integer specified by `object`. If index is not specified, 0 will be used. To set an integer object, specify a value. For example, to set the first instance of the user definable integer `cpc4400:cpc4400UsrVarInteger` to the value *1234,* enter the following:

```
# idbu32 cpc4400:cpc4400UsrVarInteger 0 1234
```

To display this value, enter the following:

```
# idbu32 cpc4400:cpc4400UsrVarInteger 0
```

This will yield: `1234`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

SNMP Configuration

For more information, see “Simple Network Management Protocol” on page 261, and RFCs 2571-2575.

Delete an Entry from the SNMP Notify Filter Table

Synopsis

`snmp notify filter delete <subtree>`

where

`subtree` is an OID specified in dotted-decimal notation

Description

Delete the SNMP notify filter specified by “subtree”.

Configure an Entry in the SNMP Notify Filter Table

Synopsis

`snmp notify filter set <subtree> <mask> <type>`

where

`subtree` is an OID specified in dotted-decimal notation

`mask` is an OID mask in dotted-decimal form

`type` is a keyword: `other`, `volatile`, `nonVolatile`, `permanent`, or `readOnly`.

Description

Set up an SNMP Notify Filter entry. The parameters are:

`subtree` The MIB subtree which, when combined with the corresponding mask, defines a family of subtrees that is included in or excluded from the filter profile.

`mask` The bit mask which, in combination with the corresponding subtree, defines a family of subtrees that is included in or excluded from the filter profile.

Each bit of this bit mask corresponds to a sub-identifier of “subtree,” with the most significant bit of the i-th octet of this octet string value (extended if necessary, see below) corresponding to the (8*i - 7)-th sub-identifier, and the least significant bit of the i-th octet of this octet string corresponding to the (8*i)-th sub-identifier, where i is in the range 1 through 16.

Each bit of this bit mask specifies whether or not the corresponding sub-identifiers must match when determining if an OBJECT IDENTIFIER matches this family of filter subtrees; a “1” indicates that an exact match must occur; a “0” indicates “wild card,” i.e., any sub-identifier value matches.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Thus, the OBJECT IDENTIFIER X of an object instance is contained in a family of filter subtrees if, for each sub-identifier of the value of snmpNotifyFilterSubtree, either:

- the i-th bit of “mask” is 0, or
- the i-th sub-identifier of X is equal to the i-th sub-identifier of the value of snmpNotifyFilterSubtree.

If the value of this bit mask is M bits long and there are more than M sub-identifiers in the corresponding instance of snmpNotifyFilterSubtree, then the bit mask is extended with 1’s to be the required length.

Note that when the value of this object is the zero-length string, this extension rule results in a mask of all-1's being used (i.e., no “wild card”), and the family of filter subtrees is the one subtree uniquely identified by the corresponding instance of snmpNotifyFilterSubtree.

`mask` - This object indicates whether the family of filter subtrees defined by this entry is included in or excluded from a filter. The value is either “included” or “excluded.”

Display an SNMP Notify Filter Table

Synopsis

`snmp notify filter show`

Description

Show the SNMP Notify Filter table.

Delete an Entry from the SNMP Notify Profile Table

Synopsis

`snmp notify profile delete <name>`

where

`name` is an ASCII String.

Description

Delete the SNMP Notify Profile specified by `name`.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Up an SNMP Notify Profile Table

Synopsis

`snmp notify profile set <name> <storage>`

where

`name` is an ASCII Label.

`storage` is a keyword: `other`, `volatile`, or `nonVolatile`.

Description

Configure an entry in the SNMP Notify Profile Table. The arguments are:

`name` The name of the filter profile to be used when generating notifications using the corresponding entry in the SNMP Target Address Table.

`storage` one of the following values: “other”, “volatile”, or “nonVolatile”.

Display the SNMP Notify Profile Table

Synopsis

`snmp notify profile show`

Description

Show the SNMP Notify Profile table.

Delete an Entry from the SNMP Notify Table

Synopsis

`snmp notify table delete <name>`

where

`name` is an ASCII Label.

Description

Delete the entry specified by `name` from the SNMP Notify Table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Configure an Entry in the SNMP Notify Table

Synopsis

`snmp notify table set <name> <tag> <type> <storage>`

where

`name`	is an ASCII Label.
`tag`	is an ASCII Label
`type`	is a keyword, either `trap` or `inform`.
`storage`	is a keyword: `other`, `volatile`, or `nonVolatile`.

Description

Setup an SNMP Notify Table entry. The parameters are:

`name`	The locally arbitrary, but unique identifier.
`tag`	This object contains a single tag value which is used to select entries in the SNMP Target Address Table. Any entry in the SNMP Target Address Table which contains a tag value which is equal to the value of an instance of this object is selected. If this object contains a value of zero length, no entries are selected.
`type`	This object determines the type of notification to be generated for entries in the SNMP Target Address Table selected by the corresponding instance of SNMP Notify Tag. The value must be either “trap” or “inform”.
`storage`	One of the following values: “other”, “volatile”, or “nonVolatile”.

Display Entries in the SNMP Notify Table

Synopsis

`snmp notify table show`

Description

Show all the entries in the SNMP Notify Table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Delete an Entry from the SNMP Target Address Table

Synopsis

`snmp target address delete <name>`

where

`name`	is an ASCII Label

Description

Remove the specified entry from the SNMP Target Address table.

Configure an Entry in the SNMP Target Address Table

Synopsis

`snmp target address set <name> [ip] [port] <timeout> <retry> <taglist> <parameters> <storage>`

where

`name`	is an ASCII Label
`ip`	is an IP Address (see “IP Address” on page 74.)
`port`	is an integer value
`timeout`	is a decimal integer value, in hundreds of seconds
`retry`	is an integer value
`taglist`	is an ASCII String
`parameters`	is an ASCII String
`storage`	is a keyword: `other`, `volatile`, or `nonVolatile`.

Description

Set up an SNMP Target entry. The arguments are as follows:

`name`	A unique name to identify this entry.
`ip`	the IP address.
`port`	the UDP port number.
`timeout`	This variable should reflect the expected maximum round trip time for communicating with the transport address defined by this row. When a message is sent to this address, and a response (if one is expected) is not received within this time period, an implementation may assume that the response will not be delivered.
`retry`	This variable is the default number of retries to be attempted when a response is not received for a generated message.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

taglist	This variable contains a list of tag values which are used to select target addresses for a particular operation.
parameters	The value of this variable identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.
storage	one of the following values: “other”, “volatile”, or “nonVolatile”.

Display the Entries in the SNMP Target Address Table

Synopsis

snmp target address show [name]

where

name	is an ASCII string

Description

Show the entire SNMP Target Address table. If a name is specified, the tag list for the specified entry is displayed.

Delete an Entry from the SNMP Target Parameters Table

Synopsis

snmp target parameters delete <name>

where

name	is an ASCII string

Description

Remove the entry specified by name from the SNMP Target Parameters table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set an Entry in the SNMP Target Parameters Table

(For additional information, refer to RFC 2571 - 2573.)

Synopsis

`snmp target parameters set <name> <model> <security_model> <security_name> <security_level> <storage>`

where

`name` is an ASCII String

`model` is an ASCII String

`security_model`
is an ASCII String

`security_name`
is an ASCII String

`security_level`
is an ASCII String

`storage` is a keyword: `other`, `volatile`, or `nonVolatile`

Description

Setup an SNMP Target Parameter entry. The parameters are:

`name` a unique name to identify this entry.

`model` The Message Processing Model to be used when generating SNMP messages using this entry.

`security_model`
The Security Model to be used when generating SNMP messages using this entry.

`security_name`
The Security Name that identifies the Principal on whose behalf SNMP messages will be generated using this entry.

`security_level`
The Security level for this entry. It must be one of the following values: “noAuthNoPriv”, “authNoPriv”, or “authPriv”

`storage` one of the following values: “other”, “volatile”, or “nonVolatile”.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display the SNMP Target Parameters Table

Synopsis

`snmp target parameters show`

Description

Show the entire SNMP Target Parameters table.

Set the SNMP Community Name and Permissions

Synopsis

`snmp community set <community> [perm]`

where

`community` is an ASCII Label of up to 16 characters.

`perm` is an optional argument specifying the desired permissions. It is specified on the command line with the following keywords:

- *`rw`* specifies Read and Write permissions
- *`ro`* specifies Read Only permissions

Description

Create and set the permissions for the community name. If the community name exists, the permission is updated. If no configuration arguments are provided, the current status is displayed.

Remove SNMP Community

Synopsis

`snmp community delete <community>`

where

`community` is an ASCII Label of up to 16 characters.

Description

Delete an SNMP community entry.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display SNMP Community Entry

Synopsis

`snmp community display [community]`

where

`community` is an ASCII Label of up to 16 characters.

Description

Display an SNMP community entry. If community is not specified, all community entries are displayed.

SNMP Version 3 Commands

The following SNMP Version 3 commands are only available in Firmware 5.6 or above.

Add SNMP User

Synopsis

`snmp user add <username> <authtype> <privtype> [authkey] [privkey]`

where

`username` may be up to 32 bytes long

`authtype` Authentication type, may be md5, sha, or none

`privtype` Privacy (encryption) type, may be des or none

`authkey` is required if the *`authtype`* parameter is md5 or sha. Keys are entered as a pass phrase, from 8 to 48 bytes long. If the pass phrase contains spaces, it should be enclosed in quotes.

`privkey` is required if the *`privtype`* parameter is des. DES privacy encryption requires a key consisting of 32 hex digits (16 bytes). Keys are entered as a pass phrase, from 8 to 48 bytes long. If the pass phrase contains spaces, it should be enclosed in quotes.

Description

Adds a new SNMP Version 3 user.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Notes:

- *If a `vacmSecurityToGroupTable` entry for the user does not already exist, one will be added with the default access 'initial'. This provides read and write access to all supported MIBs for authNoPriv and authPriv users, and read only access to the MIB-II system group for noAuthNoPriv users.*
- *This command will localize the pass phrases into local keys. This process is compute extensive and may take up to 30 seconds to complete. During this time network performance may be affected. Only the localized keys are stored in the configuration files.*
- *One of the parameters to localize the pass phrases is the Engine ID, which includes the MAC address of the management port. This means that if a configuration file (**persist**, **durable**, or **running.cli**) is copied to another switch, all users will have to be deleted and added again.*
- *The switch accepts pass phrases from 8 to 48 bytes long. The user must verify their SNMP host program can accept pass phrases of the configured length. Note that longer pass phrases are usually more secure.*
- *A maximum of 32 entries are allowed.*
- *It is not possible to change the parameters for an existing user, but an existing user can be deleted and added with the new parameters.*

Delete SNMP User

Synopsis

```
snmp user delete <username>
```

Description

Deletes an existing SNMP Version 3 user.

Display SNMP Users

Synopsis

```
snmp user show [username]
```

Description

Displays all the existing SNMP Version 3 users. If `username` parameter is supplied, only that user is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Add SNMP View Entry

Synopsis

`snmp view add <viewname> <subtree> <mask> <viewtype>`

where

`viewname`	may be up to 32 bytes long.
`subtree`	may be up to 48 bytes long. Although most of the switch's supported MIBs are in the IETF tree (.1.3.6), the LAG MIB is in the IEEE tree (.1.2.840.10006). Any user defined views should take this in account.
`mask`	may be up to 16 bytes long. It is entered as a string of Hex digits.
`viewtype`	is either 'include' or 'exclude'. If a view consists of both include and exclude entries, the exclude entries should be entered first.

Description

Adds a new SNMP Version 3 `vacmViewTreeFamilyTable` entry.

Notes:

- *A maximum of 32 entries are allowed.*
- *Multiple view entries with the same name may be defined with different subnets.*

Delete SNMP View

Synopsis

`snmp view delete <viewname>`

Description

Deletes an existing SNMP Version 3 `vacmViewTreeFamilyTable` entry. The default views 'internet', 'sysview', and 'nothing' must not be deleted.

Show SNMP Views

Synopsis

`snmp view show [viewname]`

Description

Displays all the existing SNMP Version 3 views. If `viewname` parameter is supplied, only that view is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Add SNMP Access

Synopsis

snmp access add <accessname> <level> <match> <readview> <writeview> <notifyview>

where

accessname	may be up to 32 bytes long.
level	is either ‘noAuthNoPriv’, ‘authNoPriv’, or ‘authPriv’. This specifies the minimum user security level for which this access applies.
match	is either ‘exact’ or ‘prefix’
readview	may be up to 32 bytes long and must already exist in the `vacmViewTreeFamilyTable`.
writeview	may be up to 32 bytes long and must already exist in the `vacmViewTreeFamilyTable`.
notifyview	may be up to 32 bytes long and must already exist in the `vacmViewTreeFamilyTable`.

Description

Adds a new SNMP Version 3 `vacmAccessTable` entry.

Notes:

- *A maximum of 32 entries are allowed.*
- *Multiple access entries with the same name may be defined with different security levels.*

Delete SNMP Access

Synopsis

snmp access delete <accessname>

Description

Deletes an existing SNMP Version 3 `vacmAcessTable` entry. The default access ‘initial’ must not be deleted. It allows full access to authNoPriv and authPriv users, and read only access to the MIB-II system group.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Show SNMP Access

Synopsis

`snmp access show [accessname]`

Description

Displays all the existing SNMP Version 3 accesses. If `accessname` parameter is supplied, only that access is displayed.

Add SNMP Group

Synopsis

`snmp group add <groupname> <accessname>`

where

`groupname` may be up to 32 bytes long

`accessname` may be up to 32 bytes long and must already exist in the VacmAccessTable

Description

Adds a new SNMP Version 3 `vacmSecurityToGroupTable` entry.

Notes:

- *All configured SNMP Version 3 users must have an entry in this table*
- *A maximum of 32 entries are allowed*

Delete SNMP Group

Synopsis

`snmp group delete <groupname>`

Description

Deletes an existing SNMP Version 3 `vacmSecurityToGroupTable` entry.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Show SNMP Group

Synopsis

```
snmp group show [groupname]
```

Description

Displays all the existing SNMP Version 3 groups. If `groupname` parameter is supplied, only that group is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Spanning Tree Management

The CPC441x supports both 802.1D-1998, Spanning Tree Protocol (STP), and 802.1D-2004, Rapid Spanning Tree Protocol (RSTP). Many of the CLI commands are common to both, but some apply only to STP or RSTP, and are labeled as such in the following section. In addition, “Fast Port” and “Fast Uplink,” enhancements to STP that are not covered by the IEEE standard, do not apply to RSTP.

Set Spanning Tree Version

Synopsis

`span version [version number]`

where

`version number`
: is either 0 (indicating 802.1D-1998, STP), or 2 (indicating 802.1D-2004, RSTP). Values other than 0 or 2 are not accepted. The default is 0 (STP).

Description

Allows the user to select either the STP or the RSTP algorithm and protocol on power-up. By default, STP (version 0) is selected and the IEEE 802.1D-1998 algorithm runs on the switch. In order to run 802.1D-2004, RSTP, the user needs to set the version to “2”, save the configuration and reboot the switch. The following commands will run the 802.1D-2004 RSTP algorithm and protocol:

```
# span version 2
# save
# switch reset
```

When running RSTP (version 2), the switch interoperates with both 802.1D-1998 STP and 802.1D-2004 RSTP devices. If legacy switches (STP version 0) are detected on a switch port, this port automatically switches over to run STP version 0. Other ports that are not connected to legacy STP switches will continue to run the RSTP protocol. The “span version” command lets the user choose to run either the RSTP or the legacy STP algorithm on the entire switch. By default, the switch powers up running STP (version 0); to run RSTP, the user must specifically enable it. This also means that when the switch is restored to the factory default configuration with the “switch defaults” command, it will power up running 802.1D-1998 RSTP.

If no argument is provided, then the current operational Spanning Tree version is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Spanning Tree Path Cost Style

Synopsis

`span pathcost [style]`

where

`style` is either 1, indicating 802.1D-1998 path cost style (default), or 2, indicating 802.1t path cost style.

Description

This command specifies a path cost style that is used by STP and RSTP to enforce a relationship between the port speed and the Spanning Tree path cost. By default, the IEEE 802.1D-1998 path cost style is being used. To change the path cost style, the new settings must be saved and the switch rebooted. The following commands will allow the switch to use the 802.1t path cost style:

span pathcost 2

save

switch reset

The following table describes the relationship between the link speed and the path cost as defined by IEEE 802.1D-1998, 802.1t, 802.1D-2004 and 802.1D-2001.

Table 5-9: Port Path Costs

Link Speed	Path Cost	
	Style 1	Style 2
10 Mbs	100	2 000 000
100 Mbs	19	200 000
1 Gbs	4	20 000
10 Gbs	2	2 000

If no argument is provided, display the current pathcost.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Enable or Disable Spanning Tree

Synopsis

`span bridge enable [mode]`

where

`mode` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the operation of Spanning Tree for the entire board. This will enable either the STP version or the RSTP version, depending on which is specified by the “span version” command. If no argument is provided, display the current setting.

Display or Set Spanning Tree Bridge Priority

Synopsis

`span bridge priority [priority]`

where

`priority` is an integer value representing Spanning tree Priority. For IEEE 802.1D STP, the priority can be any number between 0 and 65535. IEEE 802.1D-2004 RSTP allows the priority to be set in increments of 4096 between 0 and 61440 (e.g., 0, 4096, 8192, etc.).

Description

Set the Spanning Bridge Priority. If no argument is provided, display the current value.

Display or Set Spanning Tree Hello Time

Synopsis

`span bridge hello [hello_time]`

where

`hello_time` is a decimal integer value between 100 and 1000. The recommended value is 200 (2 seconds).

Description

Set the Spanning Bridge Hello Time in hundredths of a second. If no argument is provided, display the current value.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set Spanning Tree Forward Delay Time

Synopsis

`span bridge delay [forward_delay]`

where

`forward_delay`
: is a decimal integer value between 400 and 3000. The recommended value is 1500 (15 seconds).

Description

Set the Spanning Bridge Forward Delay Time in hundredths of a second. If no argument is provided, display the current value.

Display or Set Spanning Tree Max Age Time

Synopsis

`span bridge maxage [max_age]`

where

`max_age`
: is a decimal integer value between 600 and 4000 (6 and 40 seconds). The recommended value is 2000 (20 seconds).

Description

Set the Spanning Bridge Max Age Time in hundredths of second. If no argument is provided, display the current value.

Enable or Disable Spanning Tree Fast Uplink (STP Only)

Synopsis

`span bridge fast [enable]`

where

`enable`
: is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the operation of Fast Uplink (“Fast Uplink” on page 369) for the entire switch. If no argument is provided, display the current setting.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display Spanning Tree Status

Synopsis

```
span bridge show
```

Description

Display the following Spanning Tree status information:

Root Bridge ID, Bridge ID, Root Path Cost, Spanning Tree timer values, Spanning Tree version:

stp (0) or rstp (2). With RSTP some additional information is displayed such as Force Version and the state of the Port Protocol Migration state machine.

Port: This is a physical port number on the switch starting with 1 for the first port.

Port State: Allowable states for IEEE 802.1D STP and IEEE 802.1D-2004 STP-compatible modes are: Disabled, Listening, Learning, Forwarding and Blocking. Allowable states for the IEEE 802.1D-2004 RSTP are: Discarding, Learning, Forwarding.

Role: Allowable roles for the IEEE 802.1D STP and the IEEE 802.1D-2004 STP-compatible mode are: Designated (D) and Root (R). Allowable roles for the IEEE 802.1D-2004 RSTP mode are: Disabled (Di), Alternate (A), Backup (B), Root (R), Designated (D).

Pcost: Path Cost is a contribution of the path through this port, when the port is a Root Port, to the total cost of the path to the Root for this bridge. The port path cost may change as a result of a change in the port aggregation. In such a case, RSTP needs to recalculate the specified “ag” path cost. Two different algorithms are used to calculate the aggregated link path cost. The first one favors the maximum speed. This algorithm always assigns a better path cost to the higher-speed link. The second algorithm favors link resiliency, and assigns a better path cost to the aggregated links. The user must have an option of selecting one of the two algorithms. By default the algorithm which favors maximum speed is used. If the user selects the algorithm that favors resiliency, then he or she may also specify how many ports need to be in an aggregation before the aggregated port will have a better path cost than a higher speed link. For example, if a user selects an algorithm which favors resiliency with an argument of 4, then four 100 Mbps aggregated ports will have a better path cost than a single gigabit port. The default value of this argument is 7. That means that an aggregated link will be favored over a higher speed link if the number of ports in the aggregation is seven or more. Also, the values for the path cost for the STP and the RSTP algorithms are different. Refer to the IEEE 802.1D and the IEEE 802.1D-2004 for definitions of the path costs for the STP and the RSTP algorithms. (Also see “Port Path Cost” on page 372.)

Dcost: Designated cost. For a Designated Port, the path cost is equal to the Root Path Cost of the Bridge. Otherwise, it is a cost of the path to the Root offered by the Designated Port on the LAN to which this Port is attached.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Port Priority (Priority).
: The Port Identifier is composed of two elements: Port Priority and the Port Number. The Port Identifier is used as a tie breaker when two ports on the switch offer the same path cost to the Root Bridge and the Designated Bridge and the Designated ports for both ports are the same. In such a case, the port with a numerically lower Port Identifier wins. The default Port Priority is 128. In order to have a particular port preferred in the Root Port selection, the priority component needs to be decreased. A priority can be set between 0 and 255 (128 is a recommended default). The STP and the RSTP definition of the Port Priority are slightly different. STP assigns the upper 8 bits of the Port Identifier as the Port Priority, and therefore Port Priority can be any value between 0 and 255. RSTP assigns the upper 4 bits of the Port Identifier as the port priority, however the value is read as an 8 bit in the range 0 to 255 with the increment of 8. The allowable values are therefore: 0, 8, 16, 32, etc.

Fast Port (enabled/ disabled) (see “Fast Port” on page 369.)
: This information is not supported with RSTP. Instead, RSTP supports EdgePort, which serves a similar purpose as the STP Fast Port.

Protocol.
: This field shows whether Spanning Tree (STP/RSTP) is enabled on the port. If Spanning Tree is disabled on the port, this port will not participate in the Spanning Tree topology. If the link on such a port is up, this port will participate in the frame relay. Ports with Spanning Tree disabled will not send or receive STP BPDUs, RSTP BPDUs, GVRP BPDUs or GMRP BPDUs. It is important to understand the difference between disabling Spanning Tree globally on the switch and disabling it on the port. When Spanning Tree is disabled on the switch, then BPDUs (such as STP BPDUs, RSTP BPDUs or GARP BPDUs) are being flooded to all ports with the exception of the port on which they are received. On the other hand, when Spanning Tree is disabled on the port, this port will not send or receive any BPDUs.

Atime
: is the time (in seconds) since the last reception of a Spanning Tree BPDU (Configuration BPDU or an RSTP BPDU) on that port. If the port is Disabled or Designated, the Atime is inactive (N). In the case of an RSTP BPDU, the Atime is shown as rcvdInfoWhile/MaxAge. The rcvdInfoWhile is set to 3 x Hello_time, and is decremented by 1 every second if a BPDU is not received. The MaxAge specifies how old the message age can be before it will be discarded as too old.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Following is an example of the “span bridge show” command for Spanning Tree version 0:

```
*********************************************************************
                  STP (version 0)
RootID: 8000000331010003 BridgeID: 800000c08c086084  RPC = 19
STP ENABLED    fastUplink DISABLED  TC = NO  Top. Changes = 24
Max Age = 20, Forw. Del = 15, Hello Time = 2, Long Aging = 300
---------------------------------------------------------------------
port portState   state  Pcost  Dcost  Priority portF  Protocol ATime
---------------------------------------------------------------------
1    FORWARDING  R      19     0      128      OFF    Enabled  A 0
2    BLOCKING    B      19     0      128      OFF    Enabled  A 1
3    BLOCKING    B      19     0      128      OFF    Enabled  A 1
4    BLOCKING    B      19     0      128      OFF    Enabled  A 1
5    BLOCKING    B      19     0      128      OFF    Enabled  A 1
6    BLOCKING    B      19     0      128      OFF    Enabled  A 1
7    DISABLED    D      250    19     128      OFF    Enabled  N
8    DISABLED    D      250    19     128      OFF    Enabled  N
9    DISABLED    D      250    19     128      OFF    Enabled  N
10   BLOCKING    B      19     0      128      OFF    Enabled  A 1
11   DISABLED    D      250    19     128      OFF    Enabled  N
12   DISABLED    D      250    19     128      OFF    Enabled  N
13   DISABLED    D      250    19     128      OFF    Enabled  N
14   DISABLED    D      250    19     128      OFF    Enabled  N

15   DISABLED    D      250    19     128      OFF    Enabled  N
16   DISABLED    D      250    19     128      OFF    Enabled  N
17   DISABLED    D      250    19     128      OFF    Enabled  N
18   DISABLED    D      250    19     128      OFF    Enabled  N
19   DISABLED    D      250    19     128      OFF    Enabled  N
20   DISABLED    D      250    19     128      OFF    Enabled  N
21   DISABLED    D      250    19     128      OFF    Enabled  N
22   DISABLED    D      250    19     128      OFF    Enabled  N
23   DISABLED    D      250    19     128      OFF    Enabled  N
24   DISABLED    D      250    19     128      OFF    Enabled  N
25   DISABLED    D      250    19     128      OFF    Enabled  N
26   DISABLED    D      250    19     128      OFF    Enabled  N
---------------------------------------------------------------------
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Following is an example of the “span bridge show” command for the RSTP algorithm, version 2:

```
*****************************************************************
                  RSTP (version 2)
Spanning Tree (RSTP) is ENABLED  forceVersion = 2  RPC = 0
RootID: 8000000331010003 BrID: 8000000331010003 TC = NO  TCcnt = 0
MaxAge = 20, FwDel = 15, MesAge = 0, Hello = 2, Long Aging = 300
-----------------------------------------------------------------
port portState    Role  Pcost Dcost Priority Edge P2P Ad/Pr ATime
-----------------------------------------------------------------
1    Forwarding   D     19    0      128      NO   YES Y/Y   0/20
2    Forwarding   D     19    0      128      NO   YES Y/Y   0/20
3    Forwarding   D     19    0      128      NO   YES Y/Y   0/20
4    Forwarding   D     19    0      128      NO   YES Y/Y   0/20
5    Forwarding   D     19    0      128      NO   YES Y/Y   0/20
6    Forwarding   D     19    0      128      NO   YES Y/Y   0/20
7    Disabled     Di    19    0      128      YES  NO  N/Y   0/0
8    Disabled     Di    19    0      128      YES  NO  N/Y   0/0
9    Disabled     Di    19    0      128      YES  NO  N/Y   0/0
10   Forwarding   D     19    0      128      NO   YES Y/Y   0/20
11   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
12   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
13   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
14   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
15   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
16   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
17   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
18   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
19   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
20   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
21   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
22   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
23   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
24   Disabled     Di    19    0      128      YES  NO  N/Y   0/0
25   Disabled     Di    4     0      128      YES  NO  N/Y   0/0
26   Disabled     Di    4     0      128      YES  NO  N/Y   0/0
-----------------------------------------------------------------
D = Designated, A = Alternate, B = Backup, Di = Disabled
Ad/Pr = AdminState/ProtEnabled Atime = rcvdInfoWhile/MaxAge
```

Enable or Disable Spanning Tree Protocol on a Port

Synopsis

`span port protocol <portlist> [mode]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`mode` is a Boolean type (See “Boolean” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Enable or disable the Spanning Tree Protocol Data Unit (PDU) processing on the set of ports identified by “portlist.” If no argument is provided, the current setting is displayed. When a port has Spanning Tree disabled, the port no longer sends or receives spanning-configuration or topology-change PDUs. However, Spanning Tree will continue to include the port in calculating its active topology. It may assign a designated role to the disabled port, and place it in any of the STP states. When STP changes the port’s role, this port will transition through the Spanning Tree states. To speed up the STP port state transitions, use Fast Port (Page 369) or Fast Uplink (Page 369).

Enable or Disable a Port

Synopsis

`span port enable <portlist> [mode]`

where

`portlist`	is a List of Port numbers (see “List” and “Port” on page 74.)
`mode`	is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the operation of ports identified by “port list.” If no mode is provided, the current value is displayed. When mode is Disable, the port is placed in the Disabled Spanning Tree State. When mode is Enable, the STP State of the port is determined by the operation of the Spanning Tree Protocol.

Enable or Disable Fast Port on a Port (STP Only)

Synopsis

`span port fast <portlist> [mode]`

where

`portlist`	is a List of Port numbers (see “List” and “Port” on page 74.)
`mode`	is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable Fast Port on the specified ports. If no argument is provided, display the current value. When Fast Port is enabled on a port, the port skips over the Listening and Learning Spanning Tree states. Spanning Tree BPDUs continue to be sent on the port and BPDUs received from the port are processed. The port may enter the Blocking or Forwarding states. This command is not supported when running RSTP.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set Spanning Port Priority

Synopsis

`span port priority <portlist> [port_priority]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`port_priority` is a decimal integer value. For IEEE 802.1D, this priority value can be any number between 0 and 255. For the RSTP algorithm, this value can be set at increments of 16 between 0 and 240 (allowable values are 0, 16, 32, 48, etc.).

Description

Set the Spanning Port Priority. If no argument is provided, display the current value.

Associate Spanning Tree Enable with VLAN Creation

Synopsis

`span port vlan <portlist> [enable]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

This command causes Spanning Tree to be disabled on the specified ports after the CPC441x has completed the VLAN and IP Interface initialization step. This is useful for preventing loops until VLANs are established. This command is provided because the CPC441x runs only a single instance of the Spanning Tree protocol, not one per VLAN. See “Virtual Router Redundancy Protocol” on page 357 for an example of the use of this command.

Select Administrative Point-to-Point Mode on the Port (RSTP Only)

Synopsis

`span port pointtopoint <portlist> [mode]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`mode` is one of the following: 0 (True), 1 (False), or 2 (Auto).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

The administrative point-to-point status of the LAN segment attached to this port. A value of True (0) indicates that this port should always be treated as if it is connected to a point-to-point link. A value of False (1) indicates that this port should be treated as having a shared media connection. A value of auto (2) indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the port is configured for full duplex operation, either through autonegotiation or by management means. If no argument is specified, then this command displays both the administrative state and the operational state of the rstp point-to-point mode.

Designate Port as an Edge Port (RSTP Only)

Synopsis

`span port edgeport <portlist> [value]`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

`value` is a Boolean type: True (1), or False (2). The default value is False (2). (See “Boolean” on page 74.)

Description

Designate the specified port as an Edge port. An edge port connects directly to an end station, and does not need to transition through Listening and Learning before it becomes Designated and Forwarding. Ports that are connected to other bridges or switches must not be configured as edge ports. If a port is configured to be an edge port and the presence of another bridge or a switch is discovered on that port, then this port will not operate as an edge port. If no arguments are provided, then the current administrative and operational port state is displayed.

Force a Port to Transmit an RSTP BPDU (RSTP Only)

Synopsis

`span port force <portlist>`

where

`portlist` is a List of Port numbers (see “List” and “Port” on page 74.)

Description

When operating in the RSTP (version 2) mode, this command forces the specified ports to send RSTP BPDUs. This is useful when a legacy STP device is replaced with an RSTP device. A port that detects the presence of a legacy STP device automatically switches over to the STP mode. This port will continue to operate in STP mode even after the STP device has been removed or replaced with the RSTP device. This command can be used to restore the RSTP operation on the port after the STP device has been removed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Select RSTP Compatibility Version (RSTP Only)

Synopsis

`span rstp version [version]`

where

version is either 0 (stpCompatible) or 2 (RSTP)

Description

Selects one of two modes of operation for RSTP: stpCompatible (version = 0), or RSTP (version = 2). (This command should not be confused with “span version,” which selects either STP or RSTP.) This command is available only when the switch is running RSTP; that is, after the “span version” has been set to 2, and the switch has been rebooted. Unlike “span version,” the “span rstp version” command takes effect without rebooting. It is important to understand that even when the “span rstp version” is set to RSTP (2), the switch may still operate in stpCompatible mode (0) on those ports on which it discovers legacy 802.1D STP devices.

Set the Transmit Hold Count (RSTP Only)

Synopsis

`span rstp hold [count]`

where

`count` is an integer between 1 and 10. The default (recommended) value is 3.

Description

The Transmit Hold Count is the maximum number of BPDUs the switch can transmit per second. When the transmission counter reaches the value of the Hold Count, transmission is prohibited until the transmission counter once again becomes less than the Hold Count. The transmission counter increments by 1 for each transmission, and decrements by 1 for each second of time.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Switch Management

Reset the Switch to Factory Default Values

Synopsis

```
switch defaults
```

Description

Reboots the board and restores factory default settings that are stored in permanent memory.

Reset the Switch

Synopsis

```
switch reset
```

Description

Reboots the board without restoring factory default settings.

Display the Switch Information

Synopsis

```
switch display
```

Description

Display the switch configuration.

Enable or Disable Watchdog

Synopsis

```
switch watchdog enable [enable]
```

where

enable is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the watchdog operation on the CPC441x. If no argument is provided, display the current configuration.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Enable or Disable Reboot on Watchdog Timeout

Synopsis

`switch watchdog reboot [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the watchdog reboot on the CPC441x. If no argument is provided, display the current configuration.

Update System Files

Synopsis

`switch install <filetype> <filename>`

where

`filetype` is one of the following keywords:

`rom` to update the Boot ROM,

`appl` to update the application image,

`ipmi` to update the PM controller Application

`pmupdate` to update both the PM controller Loader and Application

`filename` is an ASCII Label of up to 40 characters specifying the file to install.

Description

Used to overwrite existing board system software with the specified *`filename`*. The *`filename`* information is displayed, including: size and checksum (CRC-32), and a confirmation is required to install the system files. If *`filetype`* is **`rom`**, then the file *`filename`* is stored into the Boot ROM. If *`filetype`* is **`appl`**, then the file *`filename`* is copied to `/CPC4400.Z`.

If *`filetype`* is `ipmi` or `pmupdate`, the firmware in the PM controller will be updated. This code is divided into two pieces: Loader and Application. The Loader portion supports the actual update process and the Application portion supports the actual PM operation. If PM program update is needed, instructions will be provided in Release Notes from Performance Technologies.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Enable or Disable Power-On Confidence (POC) Tests

Synopsis

`switch poc [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the tests for the CPC441x. If no argument is provided, the current setting is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Enable or Disable Web Management

Synopsis

`switch web [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable web management for the CPC441x. If no argument is provided, the current value is displayed.

Display Version Information

Synopsis

`switch version`

Description

Display the version of the MIB, boot software, and CPC441x application software currently installed on the switch.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Switch Security

Add a Secure Host IP Entry

Synopsis

`switch security hostip add <ip_addr> [ip_mask] <type_list> [ip_protocol] [if_descr]`

where

`ip_addr` is the host IP Address or sub-network being filtered (see “IP Address” on page 74.)

`ip_mask` is a mask that is applied to the *`ip_addr`* for a broader range in the address filtering. For a specific host, set this to 255.255.255.255. (See “IP Address” on page 74.)

`type_list` is an ASCII string consisting of one of the following:

- *`allowed`* — allow this host(s) to access the switch management.
- *`denied`* — deny this host(s) access to the switch management.

`ip_protocol` is the IP protocol the user can specify to further focus this filter criteria. If this parameter is not provided, then all protocols are included in the allowed or denied list for the specified IP Address. If a protocol is specified, then only that protocol is included in the allowed or denied list for the specified IP Address. The recognized protocols on the switch are:

- 1 ICMP
- 6 TCP
- 17 UDP

`if_descr` is the interface description of the source packets interface and can be used to further focus these filter criteria. If this parameter is not provided, then all network interfaces are included in the allowed or denied list for the specified IP Address. If an if_descr is specified, then only that network interface is included in the allowed or denied list for the specified IP Address. (See “Interface Description” on page 74.)

Description

Add a host IP address to the allowed host list or denied host list. Use optional arguments `ip_protocol` or `if_descr` for more specific optional IP filtering as desired.

Example:

```
# switch security hostip add 192.168.1.0 255.255.255.0 denied 6 mgmt0
# switch security hostip add 192.168.2.0 255.255.255.0 denied
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Notes:

- *All "denied" entries will be processed before any "allowed" entries.*
- *If only "allowed" entries are configured, this will implicitly deny everything else.*

Display the Secure Host IP Database

Synopsis

`switch security hostip show`

Example:

```
# switch security hostip add 192.168.1.0 255.255.255.0 denied 6 mgmt0
# switch security hostip show

                    SECURE HOST IP TABLE
IP            Subnet         IP            List     IP         Interface
Address       Mask           Result        Type     Protocol   Name
-------------------------------------------------------------------------
192.168.1.0   255.255.255.0  192.168.0.0   denied   6          mgmt0
```

Description

Display the current secure HostIP lists.

Delete Entries from the Secure Host IP Database

Synopsis

`switch security hostip delete <ip_addr> <ip_mask> <ip_protocol> <if_descr>`

where

`ip_addr`	is the host IP Address or sub-network being filtered (see “IP Address” on page 74.)
`ip_mask`	is a mask that is applied to the *`ip_addr`* for a broader range in the address filtering. For a specific host, set this to 255.255.255.255 (see “IP Address” on page 74.)
`ip_protocol`	can be 0 or a valid IP protocol number.
`if_descr`	can be 0 or ‘none’ or a valid interface description.

Description

Remove an entry from the allowed or denied list.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Configure Telnet Security

Synopsis

`switch security telnet [mode]`

where

`mode` is a Boolean type to indicate whether the Telnet management should be enabled. (See “Boolean” on page 74.)

- *`on`* allow Telnet access to the switch.
- *`off`* deny Telnet access to the switch.

Description

Enable or disable Telnet for the switch. If no argument is provided the current value is displayed.

Configure SNMPV1/V2c Security

Synopsis

`switch security snmpv1v2 [mode]`

where

`mode` is a Boolean to indicate whether the SNMP V1/V2C management should be enabled. (See “Boolean” on page 74.)

- *`on`* allow SNMP V1/V2C access to the switch.
- *`off`* deny SNMP V1/V2C access to the switch.

Description

Enable or disable SNMP V1/V2C for the switch. If no argument is provided the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Configure SNMPV3 Security

Synopsis

`switch security snmpv3 [mode]`

where

`mode` is a Boolean to indicate whether the SNMP V3 management should be enabled (see “Boolean” on page 74.)

- *`on`* allow SNMP V3 access to the switch.
- *`off`* deny SNMP V3 access to the switch.

Description

Enable or disable SNMP V3 for the switch. If no argument is provided, the current value is displayed.

Enable or Disable SSH

Synopsis

`sshd enable [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the Secure Shell daemon on the switch. If no arguments are provided, the current value is displayed.

Configure SSH Port Listening

Synopsis

`sshd port [port]`

where

`port` is an integer.

Description

Configure the TCP/IP port number on which SSHD listens. The default value is 22. If no port is specified, the current value is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Add a Client Public Key To the Registry

Synopsis

sshd key add [keyfile]

where

keyfile is an ASCII Label identifying the Client Key File.

Description

Client keys for SSH are stored in the directory, ‘flash:/private’. Each Key File that is in use is listed in a registry file named. id_dsa.pub, which is also located in the directory, ‘flash:/private’. This command adds a key file name to the registry file and enables the SSH Server to use the key for client authorization. The key file must be placed into the directory, ‘flash:/private’, before adding it to the registry.

Export the Host Public Key to ASCII Format

Synopsis

sshd key export [keyfile]

where

keyfile is an ASCII Label identifying the Client Key File.

Description

Export the Switch’s Public Key to Base64 Content-Transfer-Encoding. This generates an ASCII file containing the SSHD Public Host Key of the switch, allowing the key to be added to a client's known_hosts key file. The name of the output file may be provided as an argument. If no output filename is provided, the default is 'flash:/private/id_dsa.pub'. A 16-digit fingerprint of the key is displayed which may be used by the client to validate the key.

Generate New Host Public and Private Keys

Synopsis

sshd key generate

Description

Generate new public and private authentication keys for ssh. The user is prompted to enter some random text which is used to add entropy to the cryptographic algorithms used by SSH. The new key files are stored as a series of MPINTs in the files flash:/private/sshkey.pub and flash:/private/sshkey.prv. The new public key file may be exported to ASCII format with the ‘sshd key export’ command and then added to the known_hosts key file on the client machine.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Remove a Client Public Key From the Registry

Synopsis

`sshd key remove [keyfile]`

where

`keyfile` is an ASCII Label identifying the Client Key File.

Description

Client keys for SSH are stored in the directory, ‘flash:/private’. Each Key File that is in use is listed in a registry file named. id_dsa.pub, which is also located in the directory, ‘flash:/private’. This command removes a key file name from the registry file and disables the SSH Server from using it for client authorization.

Display the Client Public Keys Stored in the Registry

Synopsis

`sshd key show`

Description

Client keys for SSH are stored in the directory, ‘flash:/private’. Each Key File that is in use is listed in a registry file named. id_dsa.pub, which is also located in the directory, ‘flash:/private’. This command displays all of the currently registered Client Keys.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Thresholds

Set Rate Control Threshold

Synopsis

`threshold limit [limit]`

where

`limit` is a decimal integer in the range 1 to 262144.

Description

Set the threshold for the number of Broadcast (bcast), Multicast (mcast), or Flood (Destination Lookup Failure, DLF) frames allowed to be received and forwarded by each Port Block. A Port Block is a group of eight 10/100 ports or a single 1-gigabit port. The CPC441x has five Port Blocks: three 10/100 blocks and two 1-gigabit blocks. The three 10/100 blocks include ports 1-8, 9-15, and 16-24. The `limit` value is expressed in terms of frames per second. If no argument is provided, display the current value.

The type of frame the limit applies to is set by the Enable or Disable Threshold commands, below.

Enable or Disable Broadcast Threshold

Synopsis

`threshold bcast [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the threshold for the number of broadcast frames allowed to be forwarded by any ingress Port Block in a one second period. If no argument is provided, display the current value.

Enable or Disable Multicast Threshold

Synopsis

`threshold mcast [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Enable or disable the threshold for the number of multicast frames allowed to be forwarded by any ingress Port Block in a one second period. If no argument is provided, display the current value.

Enable or Disable Flood Threshold

Synopsis

```
threshold flood [enable]
```

where

enable is a Boolean type (See “Boolean” on page 74.)

Description

Enable or disable the threshold for the number of frames allowed to be flooded, because of a *destination lookup failure* (DLF), from any ingress Port Block in a one second period. If no argument is provided, display the current value.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

User Login Name Management

Modify User Name

Synopsis

`username [name]`

where

name is an ASCII label of up to 16 printable characters.

Description

Modify the current username used to login to the system via the serial console, Telnet, SSH and SFTP. If no argument is provided, display the current setting. The factory default is 'admin'.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

VLAN Commands

Display VLAN Status Summary

Synopsis

```
vlan status
```

Description

Display a summary of the VLAN configuration and status for the CPC441x.

Create a VLAN

Synopsis

```
vlan create  <vid> <vlan_name> [tagged] [untagged] [forbidden] [pvid]
```

where

vid	is decimal integer between 1 and 4094.
vlan_name	is an ASCII string of up to 32 characters.
tagged	is a List of Port numbers (see “List” and “Port” on page 74.)
untagged	is a List of Port numbers (see “List” and “Port” on page 74.)
forbidden	is a List of Port numbers (see “List” and “Port” on page 74.)
pvid	is a Boolean type (See “Boolean” on page 74.)

Description

Create a VLAN with specified *vid*. Optionally, a list of tagged ports, untagged ports, and forbidden ports can be added. Also, if pvid value is “true,” then the port VLAN IDs of the ports specified by “tagged” and “untagged” will be set to the VLAN ID (vid). If pvid is “false,” the port VLAN IDs will remain unchanged by the vlan create command. Pvid=true is the default; if pvid argument is omitted, the pvid of the will be the same as the vid.

Example:

```
vlan create 256 vlan256 1-2 3-6 7-8 true
```

OR

```
vlan create vid=256 vlan_name=vlan256 tagged=1-2 untagged=3-6
forbidden=7-8 pvid=true
```

Either of these commands creates a VLAN with vid=256, VLAN name of vlan256, a tagged port list of 1–2, an untagged list of 3–6, a forbidden list of 7–8, and port VLAN IDs = 256 for the tagged and untagged port. (You can also assign PVIDs independently of the VLAN Create command; see “Associate a PVID with a Set of Ports” on page 127.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set a VLAN Name

Synopsis

`vlan name <vid> [vlan_name]`

where

`vid` is decimal integer between 1 and 4094.

`vlan_name` is an ASCII Label of up to 32 characters.

Description

Set a VLAN name of an existing VLAN. If no argument is provided, display the current value.

Destroy a VLAN

Synopsis

`vlan destroy <vid>`

where

`vid` is decimal integer between 1 and 4094.

Description

Destroy a VLAN with specified `vid`.

Note: *When a VLAN is destroyed, all ports that were in that VLAN will have their respective `vid` changed according to the following:*

- *Check to see if the port is a member of any other vlans*
- *If it is not, set the `pvid` to 1*
- *If it is, assign it to the lowest untagged vlan, if no vlans use the port untagged, assign it to the lowest tagged vlan*

Destroy All VLANs

Synopsis

`vlan clear`

Description

Destroy all VLANs. Static VLAN Registration entries are removed from the FDB (Forwarding Data Base) and the RAM copy of the configuration. All ports are returned to the default VLAN.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Add Port(s) to a VLAN

Synopsis

`vlan add <vid> [tagged] [untagged] [forbidden]`

where

`vid`	is decimal integer between 1 and 4094.
`tagged`	is a List of Port numbers (see “List” and “Port” on page 74.)
`untagged`	is a List of Port numbers (see “List” and “Port” on page 74.)
`forbidden`	is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Add a port or ports to a VLAN with the specified *`vid`*. Add a list of tagged ports, untagged ports, and forbidden ports. If a port is added to one of the lists and is configured in one of the other lists, it will be automatically removed from the current list first.

It is important to first remove a port from a VLAN using the `vlan remove` command before attempting to change it between `tagged`, `untagged` or `forbidden`.

Remove Port(s) from a VLAN

Synopsis

`vlan remove <vid> [tagged] [untagged] [forbidden]`

where

`vid`	is decimal integer between 1 and 4094.
`tagged`	is a List of Port numbers (see “List” and “Port” on page 74.)
`untagged`	is a List of Port numbers (see “List” and “Port” on page 74.)
`forbidden`	is a List of Port numbers (see “List” and “Port” on page 74.)

Description

Remove port(s) from a VLAN with the specified `vid`. Remove a list of tagged ports and/or untagged ports and/or forbidden ports.

Note: *When a port is removed from a VLAN, the `vid` of the specified port will be set according to the following:*

- *Check to see if the port is a member of any other vlans*
- *If it is not, set the `pvid` to 1*
- *If it is, assign it to the lowest untagged vlan, if no vlans use the port untagged, assign it to the lowest tagged vlan*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Show VLAN Status

Synopsis

`vlan show [vid]`

where

`vid` is decimal integer between 1 and 4094.

Description

Display the member port(s) of the VLAN with the specified `vid`. Member ports are those with valid registrations for the VLAN. Display all VLANs if no *`vid`* is supplied. Identify whether the port is statically registered or dynamically registered.

The example below shows a VLAN Table for a CPC4400:

```
# vlan show

        CPC4400 VLAN TABLE

VLAN NAME                       VLAN ID             1         2
                                                    12345678901234567890123456
------------------------------------------------------------------------------
Default                                1    ----------------UUUUUUUUUU
vlan2                                  2    UUUUUUUUUMMMMMMMMFFFFFFFFFF
```

The following table identifies the symbols used in the ‘vlan show’ display:

Table 5-10: VLAN Display Legend

Symbol	Meaning	Description
-	Non-Member	The port is NOT a member of this VLAN
M	Member	The port should transmit egress packets for this VLAN as tagged. This is also the setting on a port that has been dynamically added to a VLAN due to the operation of GVRP.
F	Forbidden	The port is forbidden from ever being a member of this VLAN
U	Untagged	The port should transmit egress packets for this VLAN as untagged

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Virtual Router Redundancy Protocol (VRRP) Management

Set Interface to Participate in VRRP

Synopsis

`vrrp set <vrid> <interface> <ip_addr> [priority] [preempt] [interval] [auth]`

where

`vrid`	is an integer used to represent the virtual router identifier. The range is 1 to 255.
`interface`	is an Interface Description keyword (see “Interface Description” on page 74.)
`ip_addr`	is the IP Address that the switch is to be master or backup for.
`priority`	is an integer used to specify the priority for the virtual router. This will default to 100 if not specified. The range is 1 to 254.
`preempt`	is a Boolean type indicating whether or not this virtual router will allow itself to be preempted when acting as a master if a master with a higher priority comes on line. This will default to on if not specified. (see “Boolean” on page 74.)
`interval`	is an integer used to represent the interval, in seconds, between sending advertisement messages. This will default to 1 if not specified. The range is 1 to 255.
`auth`	is an ASCII Label used to represent the clear text password used in VRRP authentication. If no `auth` is specified, VRRP authentication will be disabled.

Description

Attach a virtual router interface to one of the logical interfaces in the CPC441x. This will initialize the router with the given values or their defaults if no values are specified. When setting up a virtual router, the priority value should be taken into consideration; a priority value of 254 is the highest currently supported. (This command will not enable the virtual router; See “Display or Set VRRP Enable” on page 255.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Delete VRRP Instance

Synopsis

`vrrp delete  <vrid> <interface>`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (see “Interface Description” on page 74.)

Description

This command will remove a VRRP server entry.

Display or Set VRRP Enable

Synopsis

`vrrp enable <vrid> <interface> [mode]`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (see “Interface Description” on page 74.)

`mode` is a Boolean type (see “Boolean” on page 74.)

Description

This command will enable or disable the specified virtual router.

Display or Set VRRP Priority

Synopsis

`vrrp priority <vrid> <interface> [priority]`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (see “Interface Description” on page 74.)

`priority` is an integer used to specify the priority to used for the virtual router. The range is 1 to 254.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

This command will set the priority of the specified virtual router. If the priority is not specified, the current value will be displayed.

Note: *If the VRRP server has ever been turned active, the value cannot be changed.*

Display or Set VRRP Preempt Mode

Synopsis

`vrrp preempt <vrid> <interface> [preempt]`

where

`vrid`	is an integer used to represent the virtual router identifier. The range is 1 to 255.
`interface`	is an Interface Description keyword (See “Interface Description” on page 74.)
`preempt`	is a Boolean type indicating whether or not this virtual router will allow itself to be preempted when acting as a master if a master with a higher priority comes on line. (See “Boolean” on page 74)

Description

This command will set the preempt mode of the specified virtual router. If the preempt mode is not specified, the current value will be displayed.

Note: *If the VRRP server has ever been turned active, the value cannot be changed.*

Display or Set VRRP Authentication Mode

Synopsis

`vrrp authtype <vrid> <interface> [authtype]`

where

`vrid`	is an integer used to represent the virtual router identifier. The range is 1 to 255.
`interface`	is an Interface Description keyword (See “Interface Description” on page 74.)
`authtype`	is one of the following: *`off`*, *`password`* or *`ip_auth`*. *`ip_auth`* is not currently supported and will return an error.

Description

This command will enable or disable authentication or set the authentication type for the specified virtual router.

Note: *If the VRRP server has ever been turned active, the value cannot be changed.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Display or Set VRRP Authentication Password

Synopsis

`vrrp password <vrid> <interface> <password>`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`password` is an ASCII Label used to represent the clear text password used in VRRP authentication. A maximum of 8 characters are allowed.

Description

This command will set the clear text password for the specified router if the specified router has the authorization type set to password.

Note: *If the VRRP server has ever been turned active, the value cannot be changed.*

Display or Set VRRP Advertisement Interval

Synopsis

`vrrp interval <vrid> <interface> [interval]`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`interval` is an integer used to represent the interval, in seconds, between sending advertisement messages. The range is 1 to 255.

Description

This command will set the advertisement interval of the specified virtual router. If the advertisement interval is not specified, it will be displayed.

Note: *If the VRRP server has ever been turned active, the value cannot be changed.*

Note: *The Advertisement Interval must be configured the same on all routers configured to backup a specific VRID.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Enable or Disable the VRRP Fast Feature

Synopsis

`vrrp fast [enable]`

where

`enable` is a Boolean type (See “Boolean” on page 74.)

Description

This option overrides the protocol specification for the VRRP advertisement interval by allowing the user to configure the advertisement interval in deciseconds instead of seconds. Enable this option prior to creating VRRP instances.

Note: *Because this option is not interoperable with VRRP implementations from other vendors, it should be used with caution.*

Display VRRP Information

Synopsis

`vrrp display [<vrid> <interface>]`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

Description

This command will display all appropriate information on the specified virtual router or all, if vrid and Interface are not specified.

Display VRRP Statistics

Synopsis

`vrrp statistics [<vrid> <interface>]`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Description

Displays all appropriate statistics on the specified virtual router. If vrid and interface are not specified, statistics for all VRRP servers will be displayed. Below is an example:

```
VRID IFace Mast AdRc IvEr AuFl PZPS IvlT AdrL IvAu AuMM PkLn
-------------------------------------------------------------
 1   sw0   0    0    0    0    0    0    0    0    0    0
```

The parameters displayed correspond to the VRRP statistics objects in RFC 2787, which provides a complete description of each. They are summarized here:

`VRID` Virtual Router ID

`IFace` Interface

`Mast (BecomeMaster)`
Number of times that this virtual router's state has transitioned to Master.

`AdRc (AdvertiseRcvd)`
Number of VRRP advertisements received by this virtual router.

`IvEr (AdvertiseIntervalErrors)`
Number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router.

`AuFl (AuthFailures)`
Number of VRRP packets received that do not pass the authentication check.

`TTLE (IpTtlErrors)`
Number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.

`PZPR (PriorityZeroPktsRcvd)`
Number of VRRP packets received by the virtual router with a priority of 0.

`PZPS (PriortyZeroPktsSent)`
Number of VRRP packets sent by the virtual router with a priority of 0.

`IvlT (InvalidTypePktsRcvd)`
Number of VRRP packets received by the virtual router with an invalid value in the 'type' field.

`AdrL (AddressListErrors)`
Number of packets received for which the address list does not match the locally configured list for the virtual router.

`IvAu (InvalidAuthType)`
Number of packets received with an unknown authentication type.

`AuMM (AuthTypeMismatch)`
Number of packets received with 'Auth Type' not equal to the locally configured authentication method.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

`PkLn (PacketLengthErrors)`
: Number of packets received with a packet length less than the length of the VRRP header.

Display or Set VRRP Master Down Interval Count

Synopsis

`vrrp interval <vrid> <interface> [interval]`

where

`vrid` is an integer used to represent the virtual router identifier. The range is 1 to 255.

`interface` is an Interface Description keyword (See “Interface Description” on page 74.)

`interval` is an integer indicating the time interval in seconds for Backup to declare Master down.

Description

Sets the interval, in seconds, between sending advertisement messages. Only the Master router sends VRRP advertisements.

The VRRP rfc2338 describes Master_Down_Interval as “Time interval for Backup to declare master down (seconds).” Calculated as: (3 x Advertisement_Interval) + Skew_time. This object allows the user to replace “3” with another integer.

Note: *Use this command with caution. It violates the VRRP Protocol, and may not be interoperable with other vendors’ implementations.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

6

Simple Network Management Protocol

Overview

This chapter describes the Simple Network Management Protocol (SNMP) Agent implementation on the CPC441x. The key topics in this chapter include:

- “SNMP Agent Overview” on page 261
- “Supported MIBs” on page 262
- “Durable MIB Parameters” on page 263
- “SNMP Trap Configuration” on page 263
- “SNMP Version 3” on page 265

SNMP Agent Overview

SNMP enables network devices, called “agents,” to be monitored, controlled, and configured remotely from a network management station (NMS). The CPC441x SNMP agent can be managed by an SNMP manager version 1, 2c, or 3.

The agent can also generate SNMPv1/2c/3-style traps in response to CPC441x events. The user may define which events should cause a trap to occur, and may also specify the client or clients that are to receive specific traps. (For information on SNMP CLI commands, see “SNMP Configuration” on page 211; for information on configuring SNMP traps, see “SNMP Trap Configuration” on page 263.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Supported MIBs

A variety of Management Information Bases (MIBs) specify the network management variables stored on the CPC441x. All mandatory parameters for the following MIBs are provided:

- EtherLike MIB – RFC 2665
- Ethernet MAU MIB – RFC 2668
- Interfaces MIB – RFC 2233
- IEEE 802.1q MIB – RFC 2674
- IEEE 802.3ad Link Aggregation MIB
- MIBII – RFC 1213
- MIBII Bridge – RFC 1493
- Performance Technologies CPC4400 Enterprise Switch MIB (applies to all CPC440x and CPC441x switches)
- Performance Technologies Enterprise IPMI PM MIB
- Performance Technologies Enterprise IPMI FRU MIB
- Performance Technologies Enterprise System MIB
- Performance Technologies Enterprise Switch MIB
- RMON – RFC 1757 (statistics, history, alarm and events)
- rmonMib.mib
- SNMP MIB – RFC 2573
- SNMP Version 3 User Security Model – RFC 2574
- SNMP Version 3 View-based Access Control Model – RFC 2575
- Wind River Master MIB

Download MIBs at http://pt.com/page/support/snmp-mibs. The Performance Technologies Enterprise MIBs are used for CPC441x-specific parameters that are not supported by the standard MIBs. ASN.1 documents defining the Performance Technologies Enterprise MIBs are provided on both the CPC441x file system and the CPC441x CD ROM, allowing SNMP clients to have complete access to the parameters supported by these MIBs.

MIB Notes

Although the RMON MIB (RFC 1757) defines the following statistics as receive-only packet counters, the silicon used on the switch implements these statistics as receive AND transmit packet counters. Separate receive or transmit packet counters are NOT available for these MIB objects.

- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

Although the Interfaces MIB (RFC 2233) defines *ifAdminStatus* as read-write, the *ifAdminStatus* is implemented as read only in the code. The user should use `oemMib:oemArchIfaceLinkAdmin` to set the up / down status of a link.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Durable MIB Parameters

"Durable" MIB parameters are restored from non-volatile Flash memory each time the board boots. Any changes to these parameters can be saved to non-volatile Flash memory by executing a "save" command from CLI, SNMP, or the Web interface.

All of the objects from the industry-standard MIB files listed above, that are writable are also durable, with the following exceptions:

- In MIBII - RFC 1213, the object *ifAdminStatus* is not supported because entries in this table include sw interfaces, which users are not permitted to administratively bring down. (Note, however, that the link state of a port interface can be brought down with *ifMauStatus*.)
- In IEEE 802.ad Link Aggregation MIB, the object *dot3addAggCollectorMaxDelay* is not supported because of a limitation within the switch silicon used for this product.

Durable CPC441x Enterprise MIB Parameters

All parameters are described in the ASN.1 MIB document, which can be found in the **.zip** file as CPC441x.mib, or on our website, http://www.pt.com. If the word DURABLE: appears in the beginning of the description section, then the element is considered to be durable as defined above.

Note: *Packet Filter configurations are not saved in the switch* ***durable*** *file and are not restored upon boot. The user must re-instantiate any User Defined Packet Filters through the use of CLI or Lua scripts invoked by* ***rc.lua****. See "Lua Programming Language" on page 449 and "File System" on page 425.*

SNMP Trap Configuration

Traps are an important network management tool, providing alerts and triggering programmed responses when anomalous or unpredictable conditions occur on the network. Configuring SNMP traps requires setting up an "SNMP target entry," i.e., configuring the SNMP agent with an IP Address to which SNMP traps should be sent.

An example of how to set up an SNMP client IP address is shown below. To do this, delete an existing entry and then re-enter it using the same name and settings, and also include the IP address you want to add. (See "SNMP Configuration" on page 211 for SNMP commands.)

```
snmp target address# delete "nms v1"
snmp target address# set "nms v1" 147.139.3.39 162 1500 3 "rfc1493
rfc1757 rfc1907 rfc2233 gemstone" "v1 params" "nonVolatile"
```

In this example, the client at 147.139.3.39 will receive all traps defined in the MIBs associated with RFC 1493, RFC 1757, RFC 1907, RFC 2233, and the Performance Technologies proprietary MIB. The Performance Technologies proprietary MIB traps are internally grouped under the tag name "tmscom".

Use the "show" command to display a table similar to the following, where the IP address and Port number are shown as a single 6-byte hexadecimal number:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
snmp target address# show

                                  Retry               Storage
Name      Address         Timeout Count   Params      Type          Status
-------------------------------------------------------------------------------
nms v10   x938b032700a2   1500    3       v1 params   nonVolatile   active
nms v20   x000000000000   1500    3       v2 params   nonVolatile   notReady
nms v30   x000000000000   1500    3       v3 params   nonVolatile   notReady
```

To display a taglist for an entry, use the following command:

```
snmp target address# show {name}
```

As in this example:

```
snmp target address# show "nms v1"
Tag list for "nms v1":
rfc1493 rfc1757 rfc1907 rfc2233 tmscom
```

Traps Supported

Among the traps currently supported are two private enterprise traps: Integrity Test traps, and User-Defined traps. Load the ptiSystem.mib in your MIB browser to see the variable binding definitions for User-Defined traps. An integrity test trap can be sent to the SNMP client as a result of an integrity test failure. If you are capturing integrity test traps, the ptiSwitch.mib should be loaded in your MIB browser so the variable bindings are defined in this MIB. User-Defined traps allow customized SNMP client notifications, using the objects in the cpc4400CommonUserDefinedTrap Table. User-defined traps can be configured through either SNMP or a LUA script. See “Examples” on page 450 for a sample Lua script.

Private:

- cpc4400:cpc4400IntegrityTestID
- cpc4400:cpc4400CommonUserDefined

RFC 1213:

- coldStart
- linkDown
- linkUp

RFC 1493:

- newRoot
- topologyChange

RFC 1757:

- risingAlarm

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Link Trap Throttle

In order to prevent overloading a network with link change traps, the CPC441x employs a throttle mechanism that limits the number of link up or link down traps that may be reported in any given 5-second period. Because this may result in lost notifications if link changes occur too quickly, the user should not depend solely on traps to provide link state information to a network management agent. It is recommended that a polling mechanism be utilized in addition to traps.

SNMP Version 3

SNMP Version 3 addresses several of the security flaws present in SNMP Versions 1 and 2. SNMP Version 3 security is based on user, instead of the community name used in SNMP Versions 1 and 2. Each SNMP Version 3 user may use either MD5 or SHA authentication, and DES privacy encryption. The use of DES privacy encryption requires either MD5 or SHA authentication. SNMP Version 3 users may be added via the CLI, or by SNMP commands. See the following SNMPv3 User CLI commands:

- “Add SNMP User” on page 219
- “Delete SNMP User” on page 220
- “Display SNMP Users” on page 220

Adding an SNMPv3 User

When adding an SNMP Version 3 user via SNMP, the following rules apply:

- The new user must have the same authentication and privacy algorithms as an existing user.
- The new user’s authentication and privacy keys can then be changed.
- The algorithms cannot be changed.
- The new user must also be added to the RFC 2575 Security to Group Table.

Note: *A maximum of 32 SNMP Version 3 user entries are allowed.*

Examples

The following example uses the open source “NET-SNMP” package to add a new SNMP Version 3 user “newdesuser” which is copied from the existing user “initialdes”.

Note: *All these commands are actually entered on a single line.*

This command adds the new user ‘newdesuser’ to the RFC2575 Security to Group Table.

```
snmpvacm -v3 -l authNoPriv -u initialsha -a SHA -A initialsha <IP
address of Switch> createSec2Group 3 newdesuser initial
```

This command adds the new user ‘newdesuser’ as a clone of the existing user ‘initialmd5des’.

```
snmpusm -v3 -l authNoPriv -u initialsha -a SHA -A initialsha <IP address
of Switch> create newdesuser initialmd5des
```

This command changes the MD5 authentication key for the user ‘newdesuser’ to ‘newauthkey.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
snmpusm -v3 -l authPriv -u initialmd5des -a MD5 -A initialmd5des  -x
DES -X initialmd5des -Ca <IP address of Switch> passwd initialmd5des
newauthkey newdesuser
```

This command changes the DES privacy encryption key for the user ‘newdesuser’ to ‘newprivkey’.

```
snmpusm -v3 -l authPriv -u initialdes -a MD5 -A initialmd5des -x DES -
X initialmd5des -Cx <IP address of Switch> passwd initialmd5des
newprivkey newdesuser
```

Default SNMP Version 3 Users

Table 6-1: “Default SNMP Version 3 Users” lists the SNMP Version 3 users that included in the default configuration. For increased security, it is strongly suggested they be deleted after configuring the Switch. We also recommend disabling SNMP versions 1 and 2, see “Configure SNMPV1/V2c Security” on page 243.

Table 6-1: Default SNMP Version 3 Users

User	Description	Authentication Key	Encryption Key
initialnone	no authorization and no encryption	none	none
initialmd5des	MD5 authentication and DES privacy encryption	initialmd5des	initialmd5des
initialshades	SHA authentication and DES privacy encryption	initialshades	initialshades
initialmd5	MD5 authentication and no privacy encryption	initialmd5	none
initialsha	SHA1 authentication and no privacy encryption	initialsha	none

SNMPv3 Security

This section describes how to set up the MG-SOFT® MIB Browser to take advantage of the CPC441x SNMPv3 security feature.

To create a new user for MG-SOFT:

1. Go to SNMP Protocol Preferences and select **SNMPv3**.
2. Click **Add User**.
3. Enter a name for this setup in the **User Profile Name** field.
4. In the **Security User Name** field, type `initialmd5`.
5. Make no changes to **Context Name** (should be blank), **Context Engine ID** (should be #), and **SNMP Port Number** (should be 161).
6. For **Authentication Protocol**, select **HMAC-MD5**.
7. Make no change to Privacy Protocol.
8. Click **Change Password** and enter `initialmd5` in the **Password** and **Password Confirmation** fields.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Note: *To use the HMAC-SHA Authentication Protocol, select it in step 6, and enter* `initialsha` *in steps 4 and 8.*

See the following SNMPv3 User CLI commands:

- “Add SNMP User” on page 219
- “Delete SNMP User” on page 220
- “Display SNMP Users” on page 220

for more information. See “SNMP Version 3” on page 265 for more information.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

7

System Management Bus and Intelligent Platform Management

Overview

This section describes the Performance Technologies System Management Bus (SMB) and Intelligent Platform Management. The key topics in this chapter include:

- “Overview of SMB” on page 269
- “Intelligent Platform Management Interface (IPMI)” on page 270
- “Local IPMI Management” on page 272
- “System-Side IPMI Management” on page 272
- “IPM Device Commands” on page 274
- “FRU Inventory Device Commands” on page 280
- “Sensor/Event Commands” on page 285
- “OEM (Vendor Specific) Commands” on page 291

Overview of SMB

The CPC441x includes Performance Technologies’ implementation of the System Management Bus (SMB). This conforms to PICMG 2.9, the specification that defines SMB in the CompactPCI environment. SMB utilizes the I^2C bus hardware layer coupled with Intelligent Platform Management software.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Intelligent Platform Management Interface (IPMI)

The Intelligent Platform Management Interface (IPMI) specification allows system components on the I^2C hardware layer bus to communicate with each other. It provides a standard interface to hardware used for monitoring a system's physical characteristics, such as temperature, voltage, power supplies, etc. IPMI makes possible "out of band" management of a system's resources, with an emphasis on controlling "hot swap" activities.

The CPC441x supports limited Peripheral Management (PM) controller functions. The implementation that is described in this section is a CompactPCI Peripheral Management controller (PM). It supports one IPMB (IPMB0) and is designed to meet the PICMG 2.9 requirements for a Peripheral Management controller. The PM supports the mandatory and some optional IPM Device Global commands as well as the IPMI Field Replaceable Unit (FRU) Inventory commands (for the Board and Product FRU Inventory Area). A set of vendor-specific (OEM) commands are also provided to allow custom System Management Software to control reset and power functions of the card assembly. Control and Status signals unique to the CPC441x, such as POWER_GOOD, P1_BDSEL, CONTROLLER_POWER, HEALTHY, HOT_SWAP_LED, and EJECTOR_SWITCH are made available through these OEM commands. Custom System Management Software can be written to monitor the state of these signals as well as drive some of them (such as HOT_SWAP_LED and CONTROLLER_POWER). Further descriptions of these signals can be found in "OEM (Vendor Specific) Commands" on page 291

Baseboard Management Controller

The Baseboard Management Controller (BMC) is the primary management controller in an IPMI implementation. It typically resides on the System Board Computer (SBC) and provides the intelligence behind the IPMI. The BMC manages the interface between the System Management Software and the Platform Management Hardware/Firmware to provide monitoring, event logging and recovery control.

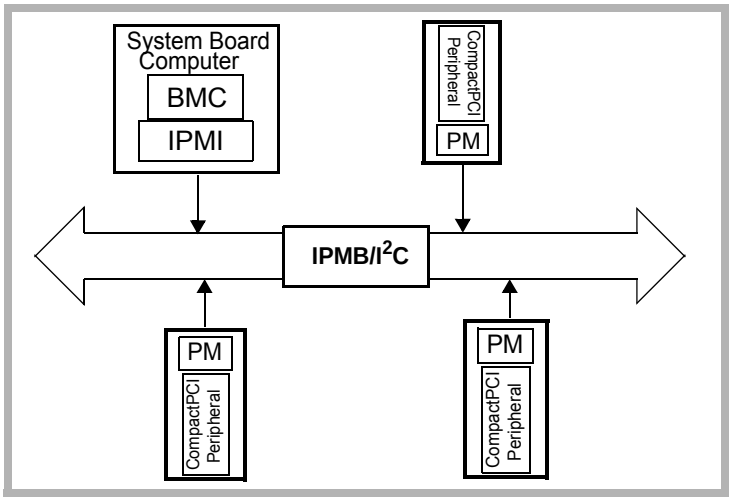
Peripheral Management Controller

The Peripheral Management Controller (PM) is a basic intelligent device that responds to mandatory "IPM Device" commands. In the Performance Technologies implementation of IPMI, the PM represents the hardware and software needed to provide the following IPMI functions:

- CompactPCI Board Host Interface
- I^2C Interface
- CompactPCI Host Port Interface Software
- IPMI Port Interface Software (IPMI/IPMB)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 7-1: CompactPCI SMB Block Diagram



Intelligent Platform Management Bus (IPMB)

The CPC441x PM implementation utilizes a single IPMB (IPMB0) that resides on the CompactPCI backplane connector P1. This bus is based on the I²C hardware layer and uses Master Write transactions only. The Baseboard Management Controller (BMC) normally sends and receives IPMI messages over the IPMB though the “Get Message” and “Send Message” commands. The IPMI commands (Requests) and Responses pass between controllers on this IPMB. IPMB Slave Addresses are determined by the CompactPCI “Geographical Address” assignment.

Table 7-1: “IPMB Slave Address Map” shows the mapping of Geographical Address and IPMB Slave Address.

Table 7-1: IPMB Slave Address Map

Geographic Address	IPMB Address	Geographic Address	IPMB Address
0	Disabled	16	D0h
1	B0h	17	D2h
2	B2h	18	D4h
3	B4h	19	D6h
4	B6h	20	D8h
5	B8h	21	DAh
6	BAh	22	DCh
7	BCh	23	DEh
8	BEh	24	E0h
9	C0h	25	E2h

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-1: IPMB Slave Address Map *(Continued)*

Geographic Address	IPMB Address	Geographic Address	IPMB Address
10	C4h	26	E4h
11	C6h	27	E6h
12	C8h	28	E8h
13	CAh	29	EAh
14	CCh	30	ECh
15	CEh	31	Disabled

IPMB Compatibility

The PM utilizes a version of IPMB that is compatible with IPMB v1.0 as it pertains to the PICMG 2.9 requirements for a Peripheral Management Controller.

Local IPMI Management

The CPU on the CPC441x provides a management interface to the IPMI subsystem to allow access to the PM through the CLI and SNMP. See “Intelligent Platform Management Interface (IPMI): Field Replaceable Unit (FRU)” on page 138 for a detailed description of the CLI commands provided to support the IPMI. For SNMP access, two enterprise MIBs allow the user to manage the data retrieved with IPMI:

- The Field Replaceable Unit (FRU) MIB (ptiIPMIFruManagement) provides FRU inventory information. The managed FRU data includes the Board and Product Inventory Areas only.
- The Program Management (PM) MIB (ptiIPMIPmManagement) manages the Globally Unique Identifier (guid), the Geographic Address (geoaddress), PM firmware upgrades, and the display of PM Statistics.

Refer to the Performance Technologies Private MIB files supplied with the CPC441x for the complete definition of these MIB objects. Two MIB ASN.1 documents are provided on the CPC441x file system and on the provided CD ROM: ptiIPMIFRU.mib and ptiIPMIPM.mib.

System-Side IPMI Management

IPMI uses message-based (Request/Response Protocol) interfaces for the Intelligent Platform Management Bus (IPMB) and for the system-side interface to the BMC. This section describes the system-side management interface supported by the CPC441x.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

IPMI Network Function Codes (netFn)

This implementation of the PM supports commands and responses with the following netFn codes, shown in Table 7-2: “Supported Network Function Codes”.

Table 7-2: Supported Network Function Codes

Name	Request	Response	Commands
Application	0x06	0x07	Get Device ID Get Self Test Results Broadcast Get Device ID Cold Reset Warm Reset Set Manufacturing Test Mode ON Get Device GUID Get ACPI Power State Set ACPI Power State
Storage	0x0A	0x0B	Get FRU Inventory Area Read FRU Inventory Data Write FRU Inventory Data
SDR	0x04	0x05	Get Device SDR Info Get Device SDR Reserve Device SDR Repository
OEM (Vendor Specific)	0x30	0x31	Diagnostic Echo Get Card Power Status Set Card Power State Get Card Power State

Completion Codes

Unless otherwise specified for a given command, standard completion code values are used. A list of these completion codes is available in the IPMI specification. The value 0x00 indicates that the “Command Completed Normally.”

IPMI Commands Supported

The following IPM/IPMI Commands are supported by the PM.

IPM Device Commands:

- Get Device ID
- Get Self Test Results
- Broadcast Get Device ID
- Cold Reset
- Warm Reset
- Set Manufacturing Test Mode ON
- Get Device GUID
- Get ACPI Power State
- Set ACPI Power State

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

FRU Inventory Device Commands:

- Get FRU Inventory Area
- Read FRU Inventory Data
- Write FRU Inventory Data

Sensor/Event Commands:

- Get Device SDR Info
- Get Device SDR
- Reserve Device SDR Repository

OEM (Vendor Specific) Commands:

- Diagnostic Echo
- Get Card Power Status
- Set Card Power State
- Get Card Power State

IPM Device Commands

This section provides detailed descriptions of the IPM Device Commands (netFn = 0x06, 0x07) supported by the PM. These commands use Network Function Codes (netFn) for Application Requests and Responses (0x06 and 0x07).

Common IPM Device Command Format

The Common IPM Device Request Message Format is outlined in Table 7-3: “IPM Device Request (Commands) Message Format”. Take note of the command byte #6, which specifies the variable for each specific function. All common Response Message functions are defined in Table 7-4: “IPM Device Response Message Format” on page 275.

There are slight differences among various commands. Each command that differs from Table 7-3: “IPM Device Request (Commands) Message Format” or Table 7-4: “IPM Device Response Message Format” on page 275 is defined in other tables under the description of that particular command.

Table 7-3: IPM Device Request (Commands) Message Format

Byte	Request Field	Description
1	rsSA	Responder’s Slave Address
2	netFn, rsLUN	NetFn = 0x06, rsLUN=0x00
3	Checksum #1	Connection Header Checksum
4	rqSA	Requester’s Slave Address
5	rqSeq, rqLUN	Sequence number and Requester’s LUN

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-3: IPM Device Request (Commands) Message Format *(Continued)*

Byte	Request Field	Description
6	Command	0x01 = Get Device ID 0x02 = Cold Reset 0x03 = Warm Reset 0x04 = Get Self Test Results 0x05 = Set Manufacturing Test Mode 0x06 = Set ACPI Power State 0x07 = Get ACPI Power State 0x08 = Get Device GUID
7	Checksum #2	Checksum of bytes 4, 5 and 6

Table 7-4: IPM Device Response Message Format

Byte	Response Field	Description
1	rqSA	Requester's Slave Address
2	netFn, rqLUN	NetFn = 0x07, rqLUN
3	Checksum #1	Connection Header Checksum
4	rsSA	Responder's Slave Address
5	rqSeq, rsLUN	Sequence number and Responder's LUN (0x00)
6	Command	0x01 = Get Device ID 0x02 = Cold Reset 0x03 = Warm Reset 0x04 = Get Self Test Results 0x06 = Set ACPI Power State 0x07 = Get ACPI Power State
7	Completion Code	
8	Checksum #2	Checksum of bytes 4 - 7

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Get Device ID

This command is used to retrieve specific information about the Intelligent Device (PM). The Request Message for this command is formatted as in Table 7-3: “IPM Device Request (Commands) Message Format” on page 274. The Response Message for the “Get Device ID” command is formatted the same as in Table 7-4: “IPM Device Response Message Format” for the first 7 bytes, with the additional response bytes formatted as shown in Table 7-5: “Get Device ID Response Message” below.

Table 7-5: Get Device ID Response Message

Byte	Response Field	Description
8	Device ID	This field is currently unspecified (0x00)
9	Device Revision	Device Rev (bits 3:0, Bit 7 = 1 (device provides SDRs))
10	Major Firmware Revision	Major Firmware Rev (bits 6:0) in binary format. AVAIL (bit 7) = 0 (Normal Operation)
11	Minor Firmware Revision	Minor FW Rev, in BCD format
12	IPMI Version	IPMI Version 1.5 (encoded 0x51)
13	IPMI Device Support	Supports FRU Inventory Device (0x08)
14-16	Manufacturer ID	Performance Technologies = 1556 (0x614) (LSB First)
17-18	Product ID	This field is currently unspecified (0x0000)
19	Checksum #2	Checksum of Bytes 4-18

Cold Reset

This command directs the Responder to perform a “Cold Reset.” This is a complete reset of all hardware, variables and interrupts to their default “power-up” values. The Self Tests will also be executed, if implemented. This is equivalent to a “Hard Reset of Card.”

The Request Message for this command is formatted as in Table 7-3: “IPM Device Request (Commands) Message Format” on page 274. The Response Message for the “Cold Reset” command is formatted as in Table 7-4: “IPM Device Response Message Format” on page 275.

Warm Reset

This command directs the Responder to perform a “Warm Reset.” The intention of this command is for the Responder to clean up its internal IPMB state. A warm reset command will reset the communications state of the IPMB. It clears the sequence numbers and retry tracking, but does not reset the IPMB interface configuration information, such as address, enables, etc.

The Request Message for this command is formatted as in Table 7-3: “IPM Device Request (Commands) Message Format” on page 274. The Response Message for the “Warm Reset” command is formatted as in Table 7-4: “IPM Device Response Message Format” on page 275.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Manufacturing Test Mode ON

This command directs the Responder to enter Manufacturing Test Mode. The response to this command only confirms that the CPC441x has accepted and processed the request. It does not provide a completion status of the tests. When this command is received, a hard reset is issued to the host processor, the POC tests will be executed once, and the switch will continue to boot. The “Get Self Tests Results” command will indicate the Pass/Fail status from the tests.

The Request Message for this command requires four parameters, and is formatted as in Table 7-6: “Set Manufacturing Test Mode ON Message Format” below. The Response Message for this command is formatted as in Table 7-4: “IPM Device Response Message Format” on page 275.

Table 7-6: Set Manufacturing Test Mode ON Message Format

Byte	Request Field	Description
1	rsSA	Responder’s Slave Address
2	netFn, rsLUN	NetFn = 0x06, rsLUN=0x00
3	Checksum #1	Connection Header Checksum
4	rqSA	Requester’s Slave Address
5	rqSeq, rqLUN	Sequence number and Requester’s LUN
6	Command	0x05 (Manufacturing Test On)
7	Parameter 1	The ‘M’ ASCII char (0x4d)
8	Parameter 2	The ‘T’ ASCII char (0x54)
9	Parameter 3	The ‘O’ ASCII char (0x4f)
10	Parameter 4	The ‘N’ ASCII char (0x4e)
11	Checksum #2	Checksum of bytes 4 - 10

Get Self Test Results

This command requests the results of the Intelligent Devices Self Test. The PM responds with “No Error” (0x55) in the Self Test Results data field in the Response Message if the self-test passed. If a self-test failure occurred, then the Self Test Results data field in the Response Message will be 0x02 (Self-Test Failed). The Additional Information field will contain test-specific failure code if the self-test failed.

The Request Message for this command is formatted as in Table 7-3: “IPM Device Request (Commands) Message Format” on page 274.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The Response Message for the “Get Self Test Results” command is formatted for the first 7 bytes as in Table 7-4: “IPM Device Response Message Format” on page 275, with the additional response bytes formatted as in Table 7-7: “Get Self Test Results Response Message” below.

Table 7-7: Get Self Test Results Response Message

Byte	Response Field	Description
8	Self Test Results	0x55 if Self-Test Passed 0x02 if Self-Test Failed
9	Additional Information	0x00 if Self-Test Passed Test Specific ErrorCode if Self-Test Failed
10	Checksum #2	Checksum of bytes 4 - 9

Set ACPI Power State

This command is issued by system software to inform a controller (the PM) of the current Advanced Configuration and Power Interface (ACPI) power state of the system. It does not actually change the ACPI power state but simply informs the PM of the state. The PM stores the ACPI Power State(s) from this command and uses the values in the Response to a “Get ACPI Power State” Command.

The Request Message for this command is formatted the same as Table 7-3: “IPM Device Request (Commands) Message Format” on page 274 for the first 6 bytes. The additional response bytes are formatted as in Table 7-8: “Set ACPI Power State Request Message” below.

Table 7-8: Set ACPI Power State Request Message

Byte	Request Field	Description
7	ACPI System Power State	See IPMI Specifications for this command
8	ACPI Device Power State	See IPMI Specifications for this command
9	Checksum #2	Checksum of bytes 4 - 8

The Response Message for the “Set ACPI Power State” command is formatted as in Table 7-4: “IPM Device Response Message Format” on page 275.

Get ACPI Power State

This command is issued by system software to retrieve the current ACPI (Advanced Configuration and Power Interface) power state from the controller (PM).

The PM Responds with the values set by “Set ACPI Power State” command. If the “Set ACPI Power State” command was not previously received, the PM will respond with “Unknown” (0x2A) in the Response data for both System and Device ACPI Power State fields.

The Request Message for this command is formatted as in Table 7-3: “IPM Device Request (Commands) Message Format” on page 274.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The Response Message for the “Get ACPI Power State” command is formatted for the first seven bytes as in Table 7-4: “IPM Device Response Message Format” on page 275, with the additional Response bytes formatted as in Table 7-9: “Get ACPI Power State Response Message” below.

Table 7-9: Get ACPI Power State Response Message

Byte	Response Field	Description
8	ACPI System Power State	See IPMI Specifications for this command
9	ACPI Device Power State	See IPMI Specifications for this command
10	Checksum #2	Checksum of bytes 4 - 9

Get Device GUID

This command directs the Responder to return the Globally Unique Identifier.This is a 128-bit identifier set at the factory. The Request Message for this command is formatted as in Table 7-3: “IPM Device Request (Commands) Message Format” on page 274. The first six bytes of the Response Message for this command are formatted as in Table 7-4: “IPM Device Response Message Format” on page 275. The remaining bytes are formatted as in Table 7-10: “Get Device GUID Response Message” below.

Table 7-10: Get Device GUID Response Message

Byte	Response Field	Description
7	Completion Code	
8-23	GUID	16 Byte GUID
24	Checksum #2	Checksum of bytes 4 - 23

Broadcast Get Device ID

This is a broadcast version of the “Get Device ID” command and is used to discover Intelligent Devices on the IPMB. The response by the PM to this command is identical to the response from the “Get Device ID” command in Table 7-4: “IPM Device Response Message Format” on page 275.

The Request Message for this command has a format similar to other Request Messages, but the order is different. The format of the “Broadcast Get Device ID” command is as follows in Table 7-11: “Broadcast Get Device IP Request Message” on page 280.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-11: Broadcast Get Device IP Request Message

Byte	Request Field	Description
1	Broadcast Address	0x00
2	rsSA	Responder's Slave Address
3	netFn, rsLUN	NetFn = 0x06, rsLUN=0x00
4	Checksum #1	Connection Header Checksum
5	rqSA	Requester's Slave Address
6	rqSeq, rqLUN	Sequence number and Requester's LUN
7	Command	0x01 = Get Device ID
8	Checksum #2	Checksum of bytes 5, 6, and 7

FRU Inventory Device Commands

This section provides detailed descriptions of the FRU Inventory Device Commands (netFn = 0x0A, 0x0B) supported by the PM. These commands use Network Function Codes (netFn) for Storage Requests and Responses (0x0A and 0x0B). The Board Info Area and the Product Info Area can be written by the IPMI "Write FRU Inventory Data" command.

Common FRU Inventory Device Commands

Common Request Message formats are outlined in the Table 7-12: "FRU Inventory Device Request Formats" on page 281. Take note of the command byte #6, which specifies the variable for each specific function. All common Response Message functions are defined in Table 7-13: "FRU Inventory Device Response Formats" on page 281.

There are slight differences among various commands. Each command that differs from Table 7-12: "FRU Inventory Device Request Formats" on page 281 or Table 7-13: "FRU Inventory Device Response Formats" on page 281 is defined in other tables under the description of that particular command.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-12: FRU Inventory Device Request Formats

Byte	Request Field	Description
1	rsSA	Responder's Slave Address
2	netFn, rsLUN	NetFn = 0x0A, rsLUN=0x00
3	Checksum #1	Connection Header Checksum
4	rqSA	Requester's Slave Address
5	rqSeq, rqLUN	Sequence number and Requester's LUN
6	Command	0x10 = Get FRU Inventory Area Info. 0x11 = Read FRU Inventory Data 0x12 = Write FRU Inventory Data
7	FRU Device ID	0x00 = Device ID

Table 7-13: FRU Inventory Device Response Formats

Byte	Response Field	Description
1	rqSA	Requester's Slave Address
2	netFn, rqLUN	NetFn = 0x0B, rqLUN
3	Checksum #1	Connection Header Checksum
4	rsSA	Responder's Slave Address
5	rqSeq, rsLUN	Sequence number and Responder's LUN (0x00)
6	Command	0x10 = Get FRU Inventory Area Info. 0x11 = Read FRU Inventory Data 0x12 = Write FRU Inventory Data
7	Completion Code	

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Get FRU Inventory Area

This command returns the size (in bytes) of the FRU Inventory Data Area on the PM. The format of the FRU Inventory Area is as described in the *IPMI Platform Management FRU Information Storage Definition V1.0 Document Revision 1.1, September 27, 1999* by Intel, Hewlett-Packard, NEC and Dell. The PM at a minimum must include the Common Header and Board Info Area. The Product Info Area can also be used to identify specific applications.

Note: *The Common, Board and Product Info Area in the PM micro-controller provide a maximum of 152 bytes of EEPROM.*

The FRU Inventory layout for this PM implementation is in Table 7-13: “FRU Inventory Device Response Formats” on page 281.

Table 7-14: FRU Inventory Layout

Address Offset	Size (Bytes)	Description
0-7	8	Common Header - Contains Offsets to other Areas
8-71	64	Board Info Area
72-151	80	Product Info Area

The Request Message for this command is formatted exactly as Table 7-12: “FRU Inventory Device Request Formats” on page 281, with the addition of one more byte definition, as in Table 7-15: “Get FRU Inventory Area Request Commands” below.

Table 7-15: Get FRU Inventory Area Request Commands

Byte	Request Field	Description
8	Checksum #2	Checksum of bytes 4 - 7

The Response Message for the “Get FRU Inventory Area Info” command is formatted as Table 7-13: “FRU Inventory Device Response Formats” on page 281, with the following additions as in Table 7-16: “Get FRU Inventory Area Response Message” below.

Table 7-16: Get FRU Inventory Area Response Message

Byte	Response Field	Description
8	FRU Inventory Area Size in Bytes (LSB)	152 bytes (0x98)
9	FRU Inventory Area Size in Bytes (MSB)	0x00
10	Access Size	0x00 - Device accessed by bytes
11	Checksum #2	Checksum of bytes 4 - 10

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Read FRU Inventory Data

This command provides the requester with a “low level” read of the FRU inventory data at the specified offset address with the specified byte count.

Note: *IPMB allows a maximum of only 32 byte messages total.*

The Request Message for this command is formatted as in Table 7-12: “FRU Inventory Device Request Formats” on page 281, with the addition of several more byte definitions, as in Table 7-17: “Read FRU Inventory Data Request Commands” below.

Table 7-17: Read FRU Inventory Data Request Commands

Byte	Request Field	Description
8	FRU Inventory Offset Address (LSB)	LS Byte of Offset from the beginning of the FRU Inventory Area to Start Reading Data
9	FRU Inventory Offset Address (MSB)	MS Byte of Offset from the beginning of the FRU Inventory Area to Start Reading Data
10	Count to Read	Must be at least 1 but no more than 23 (Bytes)
11	Checksum #2	Checksum of bytes 4 - 10

The Response Message for the “Read FRU Inventory Data” command is formatted as in Table 7-13: “FRU Inventory Device Response Formats” on page 281 with the addition of several more byte definitions, as in Table 7-18: “Read FRU Inventory Data Response Message” below.

Table 7-18: Read FRU Inventory Data Response Message

Byte	Response Field	Description
8	Count Returned	Number of Bytes Returned in the Response Data
9 to N	Requested Data	At least 1 byte but no more than 23 bytes
N+1	Checksum #2	Checksum of Bytes 4 to N

Note: *“N” in the above table refers to a byte count between 9 and 31.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Write FRU Inventory Data

This command provides the requester with a “low level” write of the FRU inventory data at the specified offset address. It allows IPMI write access to any non-write protected area in the PM FRU Inventory Area.

Note: *IPMB allows a maximum of 32-byte messages total.*

The Request Message for this command is formatted as in Table 7-12: “FRU Inventory Device Request Formats” on page 281, with the addition of several more byte definitions, as in Table 7-19: “Write FRU Inventory Data Request Commands” below.

Table 7-19: Write FRU Inventory Data Request Commands

Byte	Request Field	Description
8	FRU Inventory Offset Address (LSB)	LS Byte of Offset from the beginning of the FRU Inventory Area to Start Reading Data
9	FRU Inventory Offset Address (MSB)	MS Byte of Offset from the beginning of the FRU Inventory Area to Start Reading Data
10 to N	Data to Write	Must be at least 1 but no more than 22 (Bytes)
N + 1	Checksum #2	Checksum of bytes 4 - N

Note: *“N” in the above table refers to a byte count of between 10 and 31.*

The Response Message for the “Write FRU Inventory Data” command is formatted as in Table 7-13: “FRU Inventory Device Response Formats” on page 281 with the addition of several more byte definitions, as in Table 7-20: “Write FRU Inventory Data Response Message” below.

Table 7-20: Write FRU Inventory Data Response Message

Byte	Response Field	Description
8	Count Returned	Number of Bytes written
9	Checksum #2	Checksum of Bytes 4 - 8

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Sensor/Event Commands

This section provides detailed descriptions of the Sensor and Event Commands (netFn = 0x04, 0x05) supported by the PM. These commands use Network Function Codes (netFn) 0x04 and 0x05 for Sensor/Event Requests and Responses, respectively. Although the PM does not have any sensors, Sensor Data Records are used to provide information concerning the PM's capabilities and FRU information.

Get Device SDR Info

This command returns general information about the collection of sensors. The Request Message for this command is formatted as in Table 7-21: "Get Device SDR Info Request Message" below.

Table 7-21: Get Device SDR Info Request Message

Byte	Request Field	Description
1	rsSA	Responder's Slave Address
2	netFn, rsLUN	NetFn = 0x04, rsLUN=0x00
3	Checksum #1	Connection Header Checksum
4	rqSA	Requester's Slave Address
5	rqSeq, rqLUN	Sequence number and Requester's LUN
6	Command	0x20 (Get Device SDR Info)
7	Checksum #2	Checksum of bytes 4, 5, and 6

The Response Message for the "Get Device SDR Info" command is formatted as in Table 7-22: "Get Device SDR Info Response Message" below.

Table 7-22: Get Device SDR Info Response Message

Byte	Request Field	Description
1	rqSA	Requester's Slave Address
2	netFn, rsLUN	NetFn = 0x05, rqLUN
3	Checksum #1	Connection Header Checksum
4	rsSA	Responder's Slave Address
5	rqSeq, rsLUN	Sequence number and Responder's LUN (0x00)
6	Command	0x20 (Get Device SDR Info)
7	Completion Code	
8	Number of sensors in device for LUN this command was addressed to.	0x00 – The PM has no sensors.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-22: Get Device SDR Info Response Message *(Continued)*

Byte	Request Field	Description
9	Flags	[7] 0b – static sensor population [6:4] 000b – reserved [3] 0b – LUN 3 has no sensors [2] 0b – LUN 2 has no sensors [1] 0b – LUN 1 has no sensors [0] 0b – LUN 0 has no sensors
10	Checksum #2	Checksum of Bytes 4-9

Get Device SDR

The “Get Device SDR” command allows the population of sensors for the given LUN in the device to be listed and the associated SDR information for those sensors returned. Although the PM has no sensors, this is the mechanism in the IPMI specification for providing PM and FRU device information. The PM’s SDR repository is static and may not be added to, deleted from, or modified. Requesting Record ID 0x0000 will always provide SDR Type 12 – Management Controller Device Locator Record. Requesting Record ID 0x0001 always provides SDR Type 11 – FRU Device Locator Record.

The number in the Reservation ID field is obtained using the “Reserve Device SDR Repository” command. The Reservation ID is used to notify the requester that a record may have changed during the process of a multi-part read, and is only required for partial reads with a non-zero “Offset into record” field. The “Reservation Canceled” Completion Code will be issued in response to this command if the included Reservation ID does not match the most recent Reservation ID issued by the “Reserve Device SDR Repository” command. The Reservation ID field is ignored when the “Offset into record” is zero.

The Request Message for this command is formatted as in Table 7-23: “Get Device SDR Request Message” below.

Table 7-23: Get Device SDR Request Message

Byte	Request Field	Description
1	rsSA	Responder’s Slave Address
2	netFn, rsLUN	NetFn = 0x04, rsLUN = 0x00
3	Checksum #1	Connection Header Checksum
4	rqSA	Requester’s Slave Address
5	rqSeq, rqLUN	Sequence number and Requester’s LUN
6	Command	0x21 (Get Device SDR)
7	LSB Reservation ID	0xNNNN
8	MSB Reservation ID	
9	LSB Record ID	0x0000 returns SDR type 0x12 0x0001 returns SDR type 0x11
10	MSB Record ID	

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-23: Get Device SDR Request Message *(Continued)*

Byte	Request Field	Description
11	Offset into record	0x00 starts with the first byte of the record
12	Bytes to read	0xff means to read all bytes from the offset into the record to the end of the record.
13	Checksum #2	Checksum of bytes 4 through 12

Table 7-24: Get Device SDR Response Message

Byte	Request Field	Description
1	rqSA	Requester's Slave Address
2	netFn, rsLUN	NetFn = 0x05, rqLUN
3	Checksum #1	Connection Header Checksum
4	rsSA	Responder's Slave Address
5	rqSeq, rsLUN	Sequence number and Responder's LUN (0x00)
6	Command	0x21 (Get Device SDR)
7	Completion Code	
8	LSB of Record ID for next record	Allowed values are 0x0001 and 0xFFFF (indicating there are no additional records)
9	MSB of Record ID for next record	
10 – N	Requested bytes from record	See Table 7-27: "SDR Type 0x11 - FRU Device Locator Record" on page 289 and Table 7-28: "SDR Type 0x12 - Management Controller Device Locator Record" on page 290 for format of supported SDR types.
N+1	Checksum #2	Checksum of Bytes 4 through N

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Reserve Device SDR Repository

This command is used to obtain a Reservation ID and must be issued prior to issuing a “Get Device SDR” command. The Reservation ID is used by the “Get Device SDR” command to notify the requester that a record may have changed during the process of a multi-part read. The Request Message for this command is in Table 7-25: “Reserve Device SDR Repository Request Message” below.

Table 7-25: Reserve Device SDR Repository Request Message

Byte	Request Field	Description
1	rsSA	Responder’s Slave Address
2	netFn, rsLUN	NetFn = 0x04, rsLUN = 0x00
3	Checksum #1	Connection Header Checksum
4	rqSA	Requester’s Slave Address
5	rqSeq, rqLUN	Sequence number and Requester’s LUN
6	Command	0x22 (Reserve Device SDR Repository)
7	Checksum #2	Checksum of bytes 4 through 12

The Response Message for the Reserve Device SDR Repository is in Table 7-26: “Reserve Device SDR Repository Response Message” below.

Table 7-26: Reserve Device SDR Repository Response Message

Byte	Request Field	Description
1	rqSA	Requester’s Slave Address
2	netFn, rsLUN	NetFn = 0x05, rqLUN
3	Checksum #1	Connection Header Checksum
4	rsSA	Responder’s Slave Address
5	rqSeq, rsLUN	Sequence number and Responder’s LUN (0x00)
6	Command	0x22 (Reserve Device SDR Repository)
7	Completion Code	
8	LSB of Reservation ID	Allowed values are 0x0001 through 0xFFFF
9	MSB of Reservation ID	
10	Checksum #2	Checksum of Bytes 4 through N

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Supported SDR Types

Two Sensor Data Record formats are supported by the PM. The details of each type are given below.

SDR Type 0x11 - FRU Device Locator Record

The type 0x11 SDR is used to locate FRU information. This SDR is issued in response to a request for SDR record ID 0x0001. The format of this SDR is described in Table 7-27: “SDR Type 0x11 - FRU Device Locator Record” below.

Table 7-27: SDR Type 0x11 - FRU Device Locator Record

Byte	Field Name	Value	Description
1	Record ID LSB	0x01	The record ID is fixed and will always be reported as 0x0001.
2	Record ID MSB	0x00	
3	SDR Version	0x51	IPMI version 1.5 is supported
4	Record Type	0x11	FRU Device Locator
5	Record Length	variable	Number of remaining bytes following
6	Device Access Address	variable	Slave address of PM
7	FRU Device ID	0x01	Number identifying FRU device within PM
8	Logical-Physical/ Access LUN/ Bus ID	0x80	[7] 1b – device is a logical FRU device [6:5] 0b – reserved [4:3] 00b – LUN for FRU command [2:0] 000b – Private bus ID if bus = private, 000b if device is a logical FRU device
9	Channel Number	0x00	[7:4] 0000b –controller is on primary IPMB [3:0] 0000b – reserved
10	Reserved	0x00	
11	Device type	0x10	Logical FRU device
12	Device Type Modifier	0x00	IPMI FRU inventory
13	FRU Entity ID	0x00	Unspecified
14	FRU Entity Instance	0x60	Device relative instance number
15	OEM	0x00	Reserved for OEM use
16	Device ID String type/ length	0xc6	0xc6
17:+N	Device String	“FRU 0”	Short “ID” string for the FRU Device. 16 bytes maximum “FRU<sp>0”

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

SDR Type 0x12 - Management Controller Device Locator Record.

The type 0x12 SDR is used to identify management controllers on the IPMB, and for providing Entity and initialization information for all controllers, including the PM. This SDR is issued in response to a request for SDR record ID 0x0000. The format of this SDR is described in Table 7-28: “SDR Type 0x12 - Management Controller Device Locator Record” below.

Table 7-28: SDR Type 0x12 - Management Controller Device Locator Record

Byte	Request Field	Value	Description
1	Record ID LSB	0x00	The record ID is fixed and will always be reported as 0x0000.
2	Record ID MSB	0x00	
3	SDR Version	0x51	IPMI version 1.5 is supported
4	Record Type	0x12	Management Controller Device Locator Record
5	Record Length	variable	Number of remaining bytes following
6	Device Access Address	variable	Slave address of PM
7	Channel Number	0x00	[7:4] 0000b – reserved [3:0] 0000b – controller is on primary IPMB
8	Power State Notification / Global Initialization	0x00	Power State Notification [7] 0b – No ACPI System Power State notification required [6] 0b – No ACPI Device Power State notification required [5] 0b – Always 0 for backward compatibility [4] 0b – reserved Global Initialization [3] 0b – not applicable [2] 0b – Do not log initialization agent errors accessing this controller [1:0] 00b – Event message generation setting
9	Device Capabilities	0x08	[7] – 1b = Chassis device [6] – 1b = Bridge [5] – 1b = IPMB Event generator [4] – 1b = IPMB Event receiver [3] – 1b = FRU Inventory device [2] – 1b = SEL device [1] – 1b = SDR Repository device [0] – 1b = Sensor device
10	Reserved	0x00	
11	Reserved	0x00	
12	Reserved	0x00	
13	Entity ID	0x00	Unspecified
14	Entity Instance	0x60	Device relative instance number
15	OEM	0x00	Reserved for OEM use

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-28: SDR Type 0x12 - Management Controller Device Locator Record *(Continued)*

Byte	Request Field	Value	Description
16	Device ID String Type / Length	0xc5	0xc5
17	Device ID String	“PM 0”	Short “ID” string for the device “PM<sp> 0”

OEM (Vendor Specific) Commands

This section identifies the IPMI commands that are Vendor Specific (NetFn = 0x30-0x3f). There are currently four vendor specific commands supported by this PM. They are “Diagnostic Echo,” “Get Card Power Status,” “Get Card Power State” and “Set Card Power State.” The “Diagnostic Echo” command (Command Code = 0x01) is intended to be used to verify the proper functionality of the I^2C Bus and associated PM hardware. The “Get Card Power Status” command (Command Code = 0x10) returns a byte that contains the status of certain card power signals. The “Get Card Power State” and “Set Card Power State” commands (Command Codes 0x12 and 0x11, respectively) are used to actually determine and control the power state of the card (On or Off).

Common OEM Commands

Common OEM Command Request Message formats are outlined in Table 7-29: “Common OEM Request Commands”. Take note of the command byte #6, which specifies the variable for each specific function. All common Response Message functions are defined in Table 7-30: “Common OEM Response Commands” on page 292.

There are slight differences for various commands. Each command that differs from Table 7-29: “Common OEM Request Commands” or Table 7-30: “Common OEM Response Commands” on page 292 is defined in other tables under the description of that particular command.

Table 7-29: Common OEM Request Commands

Byte	Request Field	Description
1	rsSA	Responder’s Slave Address
2	netFn, rsLUN	NetFn = 0x30, rsLUN=0x00
3	Checksum #1	Connection Header Checksum
4	rqSA	Requester’s Slave Address
5	rqSeq, rqLUN	Sequence number and Requester’s LUN
6	Command	0x01 = Diagnostic Echo 0x10 = Get Card Power Status 0x11 = Set Card Power State 0x12 = Get Card Power State

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 7-30: Common OEM Response Commands

Byte	Response Field	Description
1	rqSA	Requester's Slave Address
2	netFn, rqLUN	NetFn = 0x31, rqLUN
3	Checksum #1	Connection Header Checksum
4	rsSA	Responder's Slave Address
5	rqSeq, rsLUN	Sequence number and Responder's LUN (0x00)
6	Command	0x01 = Diagnostic Echo 0x10 = Get Card Power Status 0x11 = Set Card Power State 0x12 = Get Card Power State
7	Completion Code	

Diagnostic Echo

This OEM command provides a means of verifying the functionality of the I^2C Bus and associated PM hardware. When a Diagnostic Echo Request is received, the PM will echo the message data content back to the Requester in the Response data fields.

The Request Message for this command is formatted as in Table 7-29: "Common OEM Request Commands" on page 291, with the addition of several more byte definitions, as per Table 7-31: "Diagnostic Echo Request Commands" below.

Table 7-31: Diagnostic Echo Request Commands

Byte	Request Field	Description
7 to N	Data to Echo	Must be at least 1 but no more than 24 (Bytes)
N + 1	Checksum #2	Checksum of bytes 4 - N

Note: *"N" in the above table refers to a byte count of between 7 and 31.*

The Response Message for the "Diagnostic Echo" command is formatted as Table 7-32: "Diagnostic Echo Response Message" with the following additions:

Table 7-32: Diagnostic Echo Response Message

Byte	Response Field	Description
8 to N	Count Returned	Must be at least 1 but no more than 24 (Bytes)
N + 1	Checksum #2	Checksum of Bytes 4 - N

Note: *"N" in the above table refers to a byte count of between 8 and 31.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Get Card Power Status

This OEM command provides the Requester with the current power status of the card. The PM will Respond with the power status of the card as determined by the POWER_GOOD signal pin on the general-purpose parallel I/O port of the PM microcontroller. This signal is generated by an on-board power management module and indicates that all voltage rails are within the specified limits. This command also reports the state of additional card status signals such as EJECTOR_SWITCH, HEALTHY, P1_BDSEL and the SMB_ENABLED signal, as shown in Table 7-33: “Bit Assignments for Card Power Status Byte” below.

Table 7-33: Bit Assignments for Card Power Status Byte

Bit	Signal	Description	Values
7	P1_BDSEL	BDSEL from the PCI Bus	0 indicates BDSEL is FALSE 1 indicates that BDSEL is TRUE
6	NC		
5	NC		
4	EJECTOR_SWITCH	Ejector Switch	0 indicates EJECTOR_SWITCH is Closed 1 indicates that EJECTOR_SWITCH is OPEN
3	HEALTHY	POWER_GOOD and no fault	0 indicates that HEALTHY is TRUE 1 indicates HEALTHY is FALSE
2	NC		
1	SMB_ENABLE	SMB (PM) Enable Switch	0 indicates SMB is Disabled 1 indicates that SMB is Enabled
0	POWER_GOOD	POWER_GOOD output from Hot-Swap Controller	0 indicates POWER_GOOD is FALSE 1 indicates that POWER_GOOD is TRUE

The Request Message for this command is formatted as in Table 7-29: “Common OEM Request Commands” on page 291, with the addition of one or more byte definitions, as per Table 7-34: “Get Card Power Status Request Message” below.

Table 7-34: Get Card Power Status Request Message

Byte	Request Field	Description
7	Checksum #2	Checksum of bytes 4 - 6

The Response Message for the “Diagnostic Echo” command is formatted as in Table 7-32: “Diagnostic Echo Response Message” on page 292 with the following additions outlined in Table 7-35: “Get Card Power Status Response Message” below.

Table 7-35: Get Card Power Status Response Message

Byte	Response Field	Description
8	Card Power Status Byte	As per Table 7-33: “Bit Assignments for Card Power Status Byte” on page 293
9	Checksum #2	Checksum of Bytes 4 - 8

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Set Card Power State

This OEM command allows the Requester to set Card Power and Control signals. The Requester can control the state of the CONTROLLER_POWER and HOT_SWAP_LED signals by setting or clearing the corresponding bits in the Request Data field, as shown in Table 7-36: “Bit Assignments for Card Power State Byte” below.

Table 7-36: Bit Assignments for Card Power State Byte

Bit	Signal	Description	Value
5	CONTROLLER_POWER	Controls the on-board power controller (On/Off) when the card is configured for SMB (PM) control of Power Up - See Jumper options in the Installation chapter.	0 turns off Controller Power 1 turns on Controller Power
4	NC		
3	HOT_SWAP_LED	Controls the hot swap LED	0 turns off the Hot Swap LED 1 turns on the Hot Swap LED
2	SMB_FAULT	Asserts the SMB Managed FAULT condition on the switch. The HEALTHY# signal on the PCIbus will be de-asserted and the FAULT LED on the faceplate will be illuminated if this bit is set. Other conditions may independently create a Fault condition on the switch such as; POC Failure, Watchdog Timeout, or Integrity Test Failure.[1]	0 turns off the SMB Managed Fault 1 turns on the SMB Managed Fault
1	SMB_RESET	Asserts the SMB Managed reset signal on the switch. This will cause the switch to be reset if the option is enabled. See Chapter 3, “Installation,” on page 45.	0 turns off the SMB Reset Signal 1 turns on the SMB Reset Signal
0	NC		

1. Note that if the switch should also be taken offline, then the SMB_RESET bit should be set in addition to this bit.

The Request Message for this command is formatted as in Table 7-29: “Common OEM Request Commands” on page 291, with the addition of two more byte definitions, as per Table 7-37: “Set Card Power State Request Message” below.

Table 7-37: Set Card Power State Request Message

Byte	Request Field	Description
7	Card Power State Byte	As per Table 7-36 on page 294
8	Checksum #2	Checksum of bytes 4 - 7

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The Response Message for the “Set Card Power State” command is formatted as Table 7-32: “Diagnostic Echo Response Message” on page 292 with the following additions outlined in Table 7-38: “Set Card Power State Response Message” below.

Table 7-38: Set Card Power State Response Message

Byte	Response Field	Description
8	Checksum #2	Checksum of Bytes 4 - 7

Get Card Power State

This OEM command returns to the Requester the Card Power and Control signals. The CONTROLLER_POWER and HOT_SWAP_LED are encoded in a single byte and returned to the Requester in the Response Data.

The Request Message for this command is formatted as in Table 7-29: “Common OEM Request Commands” on page 291, with the addition of two more byte definitions, as per Table 7-39: “Get Card Power State Request Message” below.

Table 7-39: Get Card Power State Request Message

Byte	Request Field	Description
7	Checksum #2	Checksum of bytes 4 - 6

The Response Message for the “Set Card Power State” command is formatted as Table 7-32: “Diagnostic Echo Response Message” on page 292 with the following additions shown in Table 7-40: “Get Card Power State Response Message” below.

Table 7-40: Get Card Power State Response Message

Byte	Response Field	Description
8	Card Power State Byte	As per Table 7-36 on page 294
9	Checksum #2	Checksum of Bytes 4 - 7

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

8

Web Management

Overview

This chapter describes the Web Management HTTP Server-based management entity on the CPC441x. The key topics in this chapter include:

- "HTTP Server Overview" on page 297
- "Page / Screen Navigation and Features" on page 297

HTTP Server Overview

The CPC441x supports Web-based management through an on-board web server. The web server provides access to Web pages that display the switch configuration and allow parameter modification. The Web pages provide network and switch management using industry standard Web browsers. The following Web browsers are known to work (others may also):

- Netscape Communicator 4.5 and 4.6
- Microsoft Internet Explorer 4.0 and 5.0

The CPC441x Web implementation requires a username and password to login. The username is `admin`. The password required is the same as that for access to the CLI. The default password is `password`.

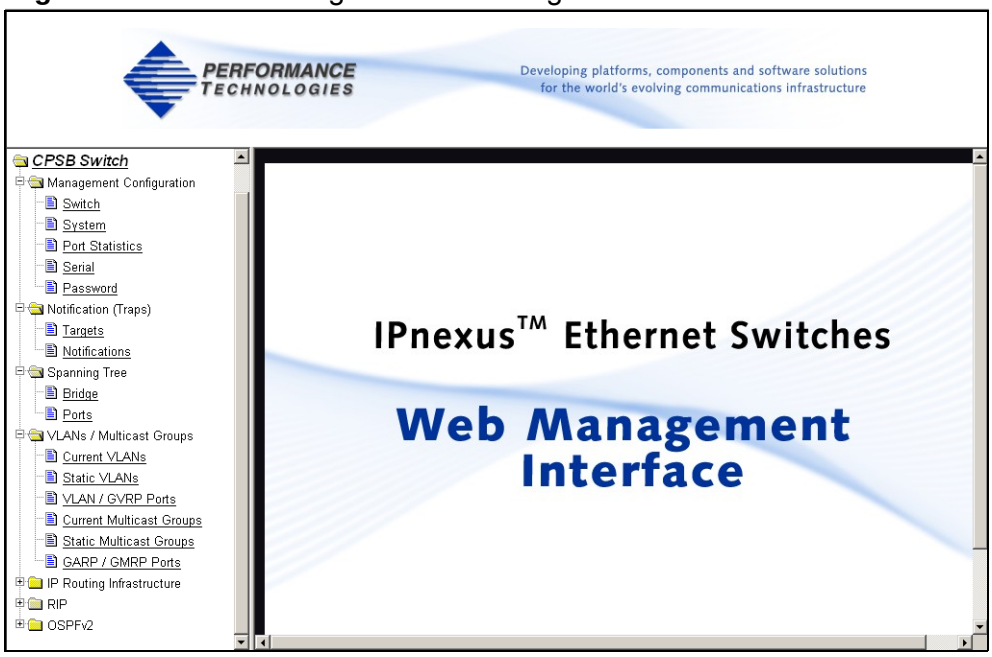
Note: *Not all parameters are configurable via the HTTP manager. The CLI and SNMP support management of all parameters.*

Page / Screen Navigation and Features

Each page is divided into two frames: the Navigation frame and the Management frame. The Switch Configuration page is shown below:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 8-1: Switch Configuration Web Page



The Navigation Bar displays the contents of Web management, grouping the Web pages in folders. To display a particular page, simply click it. Use the Tab key to advance through fields on a page, Shift+Tab to go back, or simply click a particular field with the mouse.

The following buttons are available, in varying combinations, at the bottom of Management pages:

- *Refresh:* Refreshes (updates) all fields on the page. For example, the user can select *Refresh* to update the statistics on the *Port Statistics* page.
- *Apply:* Applies the updated values on this page to the switch and/or management agent.
- *Save:* Does an *Apply* and then saves *all* configuration parameters to NVM storage. As the *Save* feature may take a while to perform (e.g., if it's necessary to erase and write Flash), it is recommended that the user make all (or many) of his/her changes before selecting *Save*.
- *Clear:* Clears the Web browser (i.e., client) fields.
- *Delete:* Deletes the current record.

If an error is found while processing the *Apply* or the *Save* button, an error message is displayed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 8-1: “Web Pages and Descriptions” summarizes the CPC441x Management web pages.

Table 8-1: Web Pages and Descriptions

Folder	Page Label	Page Title and Description
Management Configuration	Switch	Switch Configuration: Sets up basic switch parameters
	System	System Configuration: Contains MIB II System parameters plus Product Name
	Port Statistics	Port Configuration / Statistics: Provides port enable / disable and speed / duplex plus statistics
	Serial	Serial Configuration: Sets baud rate of serial console
	Password	Password Modification
Notification (Traps)	Targets	SNMP Target Addresses, SNMP Target Parameters
	Notifications	SNMP Notify Table, SNMP Notify Filter Profile Table, SNMP Notify Filter Table
Spanning Tree	Bridge	Spanning Tree Bridge Parameters: Sets up bridge-level STP parameters
	Ports	Spanning Tree Port Parameters: Sets up port-level STP parameters
VLANS / Multicast Groups	Current VLANS	Current VLAN Configuration: Displays current VLAN configuration (dynamic and static)
	Static VLANS	Static VLAN Configuration: Configures static VLAN by VID
	VLAN / GVRP Ports	VLAN / GVRP Port Configuration: Configures VLAN and GVRP port parameters
	Current Multicast Groups	Current Multicast Groups: Displays current multicast groups (dynamic and static)
	Static Multicast Groups	Static Multicast Configuration: Configures static multicast configuration by VID and MAC address
	GARP / GMRP Ports	GARP / GMRP Port Configuration

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

9

Port Configuration

Overview

This chapter contains information on configuring the CPC441x ports. The CPC441x provides twenty-four switched 10/100 Ethernet ports, two gigabit ports, and one out-of-band management 10/100 Ethernet port. All of the 10/100 Mb ports and 10/100/1000 Mb copper (CPC4416) ports support Auto-Negotiation for speed, full or half duplex, and Flow Control. The fiber gigabit ports on the CPC4411 support 1000Mb full duplex operation with Flow Control. The fiber gigabit ports support Auto-Negotiation for Flow Control (Pause) only.

The CPC441x may be managed through any of its ports. The CPC441x has up to 17 IP network interfaces. One interface is through the management port and the others are switched port interfaces. These interfaces allow external devices to communicate with the CPC441x, and also permit management of the switch through IP-based network protocols (Telnet, SNMP, HTTP, FTP, TFTP).

The key topics in this chapter include:

- "Auto Polarity Sense and Auto MDX" on page 301
- "Port Configuration" on page 302

Auto Polarity Sense and Auto MDX

The twenty-four 10/100Mb TX switched ports, and the two 10/100/1000 TX ports (CPC4416 only), have auto-polarity sense and Auto MDX. Auto MDX is the ability to swap the transmit and receive pairs if the wrong cable is used. Auto-polarity sense is the ability to swap the TX+ and TX- (or RX+ and RX-) wires if the incorrect polarity is detected. The management port does not support auto-polarity sense and Auto MDX.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Note: *The auto-polarity feature is only operational when the port is set up as Autonegotiate. See"Port Commands" on page 181 to enable or disable the Autonegotiate function.*

When Autonegotiate is enabled the following port signals and characteristics are sensed and corrected, if needed, to match the connected device:

- TX+ and TX- Polarity (Auto-polarity sense)
- RX+ and RX- Polarity (Auto-polarity sense)
- TX and RX cross-connect (Auto MDX)

Port Configuration

The Ethernet ports support the ability to configure their operational mode (speed, duplex, flow control). See "Port Commands" on page 181 for details. If the port is configured for Auto Negotiate (default), the port will advertise its full capabilities. For 10/100 ports, these are: 10M or 100M, Full or Half, Symmetric or Asymmetric Pause. For twisted-pair gigabit ports, these are: 10M, 100M, or 1000M, Full Duplex, Symmetric or Asymmetric Pause. For 1000M Fiber ports, these are Symmetric or Asymmetric Pause.

When setting the port configuration manually, all three operational parameters must be specified (speed, duplex, flow control). If you manually configure the port, you are restricted to 10M or 100M speed; 1000M requires Autonegotiation to be enabled.

Flow control is based on IEEE 802.3x PAUSE frames when the link is full duplex. Half duplex flow control is not supported.

IEEE 802.3x flow control causes the CPC441x to transmit PAUSE frames to its link partner when its buffers fill up. The link partner will not send further frames under this condition. Likewise, if the CPC441x receives a PAUSE from its link partner, it will cease to send until the overflow condition is alleviated. See the IEEE 802.3 1998 Specification, Appendix 31B.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

10

VLANs

Overview

This chapter describes how CPC441x Virtual LANs (VLANs) are configured and used. The key topics in this chapter include:

- "GVRP" on page 304
- "VLAN Identification" on page 304
- "VLAN Management" on page 305
- "VLAN Configuration" on page 305

General

The CPC441x supports the IEEE 802.1Q standard for VLANs. VLANs on the CPC441x are port-based VLANs that are created either statically under management control or dynamically through the operation of the GVRP (GARP VLAN Registration Protocol). See the IEEE 802.1Q-1998 specification for a formal definition of 802.1Q VLANs. An excellent reference is "The Switch Book: The Complete Guide to LAN Switching Technology" by Rich Seifert (May 2000), John Wiley & Sons; ISBN: 0471345865.

IEEE 802.1Q VLANs allow the construction of broadcast domains without being restricted by physical connections. A VLAN is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN).

Implementing VLANs on your network has the following advantages:

- VLANs control broadcast traffic. If a device in a particular VLAN transmits a broadcast frame, only devices in that VLAN receive the frame.
- VLANs provide extra security. Devices in a VLAN can only communicate with devices on the same VLAN.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- VLANs ease moves, adds, and changes of devices on networks. If a device in a VLAN is moved to a port in another part of the network, simply configure the new port to be in the VLAN of the moved device.

Up to 16 VLANs can be defined on the CPC441x, including all dynamically created VLANs as well as user-defined VLANs.

GVRP

GVRP (GARP VLAN Registration Protocol) is defined in IEEE 802.1Q. It is a protocol used to allow switches to exchange VLAN membership information. By running GVRP, multiple switches can learn which VLAN(s) a port is a member of. This is a very useful capability when the switch is being used for Layer-2 operation. When used as a Layer-3 switch, however, it is usually better to create static VLANs and associate them with IP network interfaces. Allowing VLAN memberships to dynamically change through the operation of GVRP may cause subnet boundaries to be crossed.

By default, GVRP is enabled on all ports of the CPC441x. To disable GVRP on selected ports, execute the following command:

```
# gvrp set <portlist> off
```

The following command will re-enable GVRP on the selected ports:

```
# gvrp set <portlist> on
```

The switch supports a command to disable the GVRP Protocol, but it is better to leave GVRP enabled on the switch and to disable its operation on the ports that are associated with Layer-3 subnets. When you disable GVRP, all GVRP Protocol Data Units received by the switch will be sent to the CPU and then replicated to all ports that have the GVRP Protocol enabled on them, i.e., the GVRP PDUs will be forwarded to all other ports. This allows other switches that are running GVRP to construct VLAN memberships. If you disable GVRP on more than one switch, but have any switch in the network running GVRP, you could expose the network to a “GVRP Storm,” caused by the enabled switch generating GVRP PDUs, and the disabled switches replicating those PDUs.

VLAN Identification

All frames that enter the CPC441x are identified as to their VLAN membership. Once the frame is identified as belonging to a particular VLAN, it may only be forwarded to other ports that are members of that VLAN. VLAN membership is determined by a VLAN Identifier (VID). The VID may be carried in the frame itself when the frame has been tagged by the source station (or a tagging switch), or the VID may be set to a default value assigned to the receiving port. The default VID assigned to a frame by the receiving port, when the frame is not already tagged, is called the Port VID or PVID. This parameter is set by management action.

Once a frame has been identified as belonging to a VLAN, it can be transmitted only to those ports that are members of that VLAN. Ports may be made members of a VLAN by management action through the creation of static VLANs, or through the operation of the GARP VLAN Registration Protocol (GVRP). GVRP is a protocol that is used between devices to announce the desire to receive frames belonging to a particular VLAN. The CPC441x participates in this protocol to create dynamic VLAN membership registrations.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Refer to the IEEE 802.1Q-1998 specification for details on the operation of GVRP and VLANs. Also, refer to RFC2674 for information regarding the management of VLANs. All of the CPC441x VLAN management interfaces are based on the MIB defined in RFC2674.

VLAN Management

Port Parameters

The primary port-based configuration parameters that affect the operation of VLANs on the CPC441x include the following:

- **PVID** - Each port is assigned a Port VLAN ID value which is used to identify the VLAN membership of frames that arrived untagged.
- **Acceptable Frame Type** - Each port may be configured to allow only tagged or untagged frames, or to allow all frames to be received.
- **Ingress Filtering** - Each port may be configured to only forward frames received on that port if the frames have been identified as members of a VLAN that the receiving port is also a member of.
- **GVRP Enable** - The operation of GVRP may be disabled on a port-by-port basis.

Static VLANs

The user may create static VLAN registration entries that permanently assign ports to particular VLANs and which also define whether frames sent on a set of ports for a particular VLAN should be sent tagged or untagged. Each static VLAN registration entry defines which ports are allowed to be members via GVRP operation, which are forbidden from a VLAN, which are permanent members of a VLAN that transmit tagged frames, and which are permanent members of a VLAN that transmit untagged frames.

VLAN Configuration

Network configurations often include some ports connected to other VLAN- aware switches and end stations, and some ports connected to VLAN-unaware switches or end stations, and some ports connected to a combination of the two. The manipulation of the port VLAN parameters and the Static VLAN Registration entries allows all of these devices to inter-operate. The following guidelines may be used to configure VLANs for a generic mixture of VLAN-aware and VLAN-unaware devices.

Note: *These are general guidelines only and may not apply to all network configurations.*

For switch ports that are only connected to “VLAN-aware” end stations and switches:

- Enable GVRP and let the devices dynamically create VLANs as needed.
- Set the PVID value to 1. In case an untagged frame does arrive on this port it will be placed in the default VLAN.

For switch ports connected to “VLAN-unaware” end stations and switches only:

- Turn off GVRP.
- All devices on these ports will be members of the same VLAN. Set the PVID of that port to the appropriate VID.
- Create a Static VLAN registration for this VLAN. Set the port to permanent untagged for this VLAN.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

For switch ports connected to a mixture of “VLAN-aware” and “VLAN-unaware” stations:

- All VLAN-unaware devices on a port will be members of the same VLAN. The switch port PVID should be set to the VID of this VLAN. The VLAN-aware devices cannot share VLAN membership with the VLAN-unaware devices. This arrangement allows frames sent to the VLAN-unaware devices to be sent on the port untagged, while frames sent to the VLAN- aware devices are sent tagged.
- Enable GVRP and let the VLAN-aware devices dynamically create VLANs as needed.
- Create a Static VLAN registration to support the VLAN-unaware devices. Set the ports to permanent untagged for this VLAN.

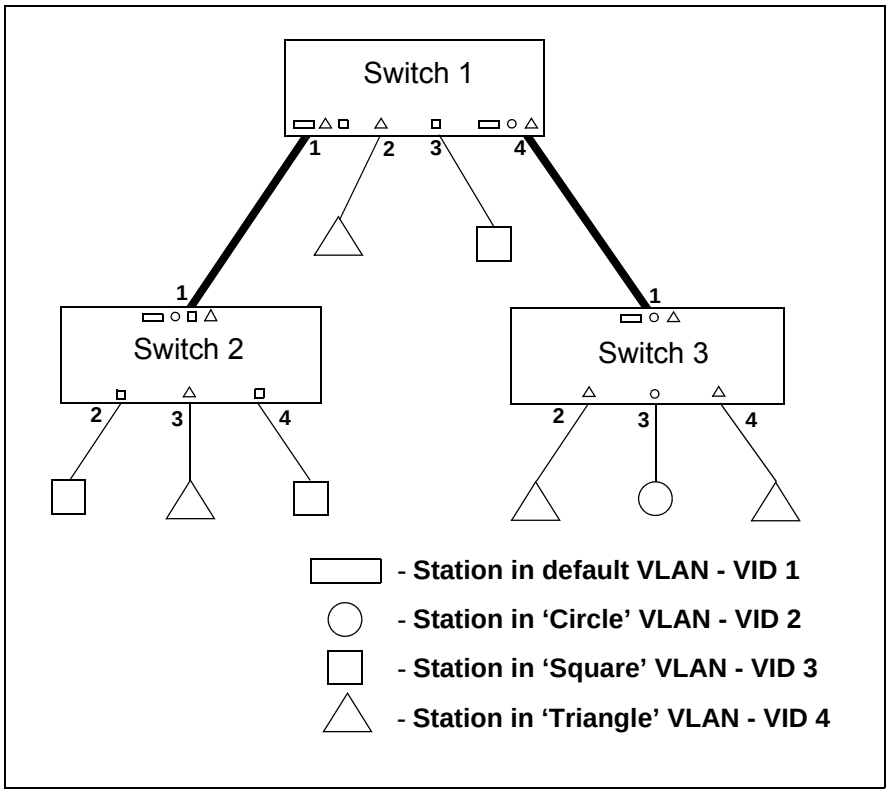
Note that the mixture case should be avoided if possible. All broadcast traffic destined to VLAN-aware devices on the port will be sent tagged and the VLAN-unaware devices will receive these frames. The network stack on these devices may not be able to deal with these frames appropriately.

Sample VLAN Configuration

Figure 10-1: “Sample VLAN Configuration” shows a sample VLAN configuration composed of three VLANs. (The CLI commands for configuring VLANs begin on “VLAN Commands” on page 250.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 10-1: Sample VLAN Configuration



In this example, the end devices are not VLAN-aware. The switches use tags on the links to the other switches to identify which VLAN a particular frame belongs to. The end station frames are tagged at the ingress ports with the PVID assigned to the port they are attached to. Management tools are used to configure the switches so that the end station frames will be tagged as they enter switch ports, the frames will travel between the switches tagged, and the tag will be removed by the switch connected to the final destination.

Ports 1 and 4 on Switch 1, port 1 on Switch 3, and port 1 on Switch 2 are all set to use GVRP to communicate VLAN membership information between the switches. These ports pass all frames tagged. The System Administrator identifies a VID for each of the VLANs. The choice is arbitrary, but must be consistent among all of the switches. The VID must be in the range 2-4094. In this example, VLAN 'circle' is assigned VID 2, VLAN 'square' is assigned VID 3, and VLAN 'triangle' is assigned VID 4.

Switch 1 is configured with a Static VLAN Registration Entry that defines a VLAN, named 'triangle', with port 2 set to be a permanent untagged port. Switch 1 also has a Static VLAN Registration Entry that defines a VLAN, named 'square', with port 3 set to be a permanent untagged port. GVRP is disabled on ports 2 and 3. The CLI commands to create this configuration are:

Switch 1

```
vlan remove vid=1 untagged=2-3
vlan create vid=4 vlan_name=triangle untagged=2
vlan create vid=3 vlan_name=square untagged=3
gvrp set 2,3 off
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Switch 2

```
vlan remove vid=1 untagged=2-4
vlan create vid=3 vlan_name=square untagged=2,4
vlan create vid=4 vlan_name=triangle untagged=3
gvrp set 2-4 off
```

Switch 3

```
vlan remove vid=1 untagged=2-4
vlan create vid=4 vlan_name=triangle untagged=2,4
vlan create vid=2 vlan_name=circle untagged=3
gvrp set 2-4 off
```

The “vlan create” command sets the PVID of the static ports to the provided VID value. The user may opt to set port PVIDs using the “gvrp pvid” command. See “Create a VLAN” on page 250 and “Associate a PVID with a Set of Ports” on page 127.

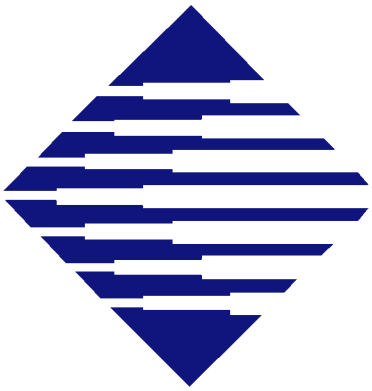
Using similar commands, Switch 2 is configured with a Static VLAN Registration Entry that defines a VLAN, named ‘square’, with ports 2 and 4 set to be permanent untagged ports and a Static VLAN Registration Entry that defines a VLAN, named ‘triangle’, with port 3 set to be a permanent untagged port. GVRP is disabled on ports 2-4.

Finally, Switch 3 is configured with a Static VLAN Registration Entry that defines a VLAN, named ‘triangle’, with ports 2 and 4 set to be permanent untagged ports and a Static VLAN Registration Entry that defines a VLAN, named ‘circle’, with port 3 set to be a permanent untagged port. GVRP is disabled on ports 2-4.

Through the operation of GVRP, port 1 on Switch 2 declares the presence of members in VLANs ‘square’ and ‘triangle’. Switch 1 registers these on its port 1. Switch 3 declares the presence of VLANs ‘triangle’ and ‘circle’ on port 1. Switch 1 registers these on port 4. Switch 1 declares the presence of VLANs ‘triangle’, ‘circle’ and ‘square’ on port 1 and Switch 2 registers these on its port 1. Switch 1 declares the presence of VLANs ‘triangle’ and ‘square’ on port 4 and Switch 3 registers these on its port 1. The registrations are indicated in Figure 10-1: “Sample VLAN Configuration” on page 307 by the small icons within the switches. The end-user ports have ‘static’ registrations.

The registrations on a port indicate which VLANs the port is a member of. Only frames that are identified as being in one of these VLANs are allowed to be transmitted onto the port.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Chapter

11

Filtering Database

Overview

This chapter describes how CPC441x Filtering Database entries are configured and used. The key topics in this chapter include:

- “Filtering Database Overview” on page 309
- “Dynamic FDB Entries and Aging Timer” on page 309
- “Permanent FDB Entries” on page 310

Filtering Database Overview

The CPC441x maintains a database of all the MAC Addresses it has learned or that have been statically configured, called the Filtering Database (FDB). The CPC441x FDB can hold up to 8191 Unicast entries and 255 Multicast entries. FDB entries for MAC Addresses that have been learned are called Dynamic Entries. FDB entries that have been created by management are called Permanent Entries.

Dynamic FDB Entries and Aging Timer

Dynamic entries are added as the switch receives frames from the network. If the Source MAC Address in a received frame is not found in the FDB, a Dynamic Entry is created for it. If, after a period of time, no additional frames are received from that Source MAC Address, the entry is removed. This period of time is the Aging Time and can be set between 1 and 1,000,000 seconds. The default is 300 seconds.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The information maintained in a Dynamic FDB Entry includes MAC Address, Learned Port Number, and VLAN Association. This information may be viewed by using the “fdb learned” command (see “Display the Dynamic Filtering Database” on page 115).

Permanent FDB Entries

Permanent Multicast MAC Entries

Multicast entries contain the MAC Address, a VID to define the VLAN that the entry applies to, a list of “forward-to” (mandatory) ports, and a list of “forbidden” (filter) ports. The “forward-to” entry defines the list of ports on which to forward frames destined to this address. The “forbidden” entry defines the list of ports on which frames destined for this address are not allowed to be sent. “Forward-to” and “forbidden” lists must be mutually exclusive. If a port is not listed in either of these fields, then the forward or filter decision is allowed to be based on the operation of GMRP.

When GMRP and/or GVRP are enabled, the number of Static Multicast entries allowed is restricted to 20 due to the overhead required to maintain GARP information. If both GVRP and GMRP are disabled, however, the number of Static Multicast entries allowed is 255. If the user disables GVRP and GMRP and then creates more than 20 Static Multicast entries, he or she will not be permitted to re-enable GVRP or GMRP until the number of Static Multicast entries is reduced to 20 or less.

Permanent Unicast MAC Entries

Unicast entries contain the MAC Address, a VID to define the VLAN that the entry applies to, and a single port that defines where to forward frames destined to this address. The switch does not support the inclusion of the ingress port in the definition of the Static Unicast database entry; the ingress port field of the RFC2764 MIB must be set to 0, which makes the static entry apply to all ingress ports. The switch also does not support the definition of multiple egress ports in a Static unicast database entry; only a single egress port is allowed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

12

Packet Filtering

Overview

This chapter describes how CPC441x Packet Filtering is configured and used. The key topics in this chapter include:

- “Applications” on page 312
- “Operation” on page 312
- “Mask Table” on page 313
- “Rules Table” on page 314
- “Matching” on page 315
- “Using Egress and Ingress Port Masks” on page 315
- “Multiple Action Execution and Conflict Resolution” on page 315
- “Management Interfaces” on page 316
- “Filter Examples” on page 316

General

The CPC441x supports a packet classification and filtering mechanism that allows the user to define special handling actions for packets based on the content of any field within the first 64 bytes of the packet.up to 32 bytes from the first 64 bytes of a packet. The 32 bytes that are inspected must be located in up to eight 4-byte groups. The groups do not need to be contiguous and the 4-byte groups do not need to be on particular byte boundaries, but the underlying hardware cannot support every combination of 32 byte groupings that are possible. The switch software will return an error indication if the underlying hardware is not capable of supporting a grouping that is specified by the user.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The switch supports up to sixteen different filters at a time. That is, you can define one filter to be the Destination IP Address and the 32nd byte of the frame, and then you can define another filter to be the Source IP Address and the 16th byte of the frame, etc.

After you have defined the filters, you may then create up to 126 different rules. Each rule defines what to do if the packet value is equal to a particular pattern. For instance, if the filter is based on Destination IP and the 32nd byte of the frame, then you can define what to do for up to 126 different values of these two fields. Note that there are 126 rules shared among all of the filters, so if you use more than one filter then you need to divide the 126 rules among them.

Based on the classification, the switch can do any of the following:

- Change the 802.1Q packet Priority.
- Forward the packet with a specific priority without changing the 802.1Q packet Priority.
- Change the IP Header TOS Precedence value.
- Send a copy of the packet to the local processor.
- Discard the packet.
- Forward the packet to a specific Egress port.
- Send a copy of the packet to a “mirrored-to” port in addition to sending it to its normal destination.

Applications

Typical applications for Packet Filtering include:

- Traffic Prioritization - Raise the priority of Voice or Video traffic to improve performance. Establish different classes of service for different users.
- Firewall - Block unwanted packets.
- Bandwidth Regulation - Prevent applications from hogging network bandwidth.
- Network Monitoring and Troubleshooting - Use filters to narrow packet mirroring for analysis.

Operation

The Packet Filter mechanism is invoked after the packet has been passed through the Ingress Port Tagging Process (for untagged packets), the Layer-2 switching process and the Layer-3 Routing Process. Any modifications made by these processes to the packet should be taken into account in building the filters. For example, all packets will have a Tag before being submitted to the Packet Filter. The value of the Tag field may have been modified due to Layer-2 switching activity. If a filter is applied to the Tag field, it will apply to the Tag value after these initial activities are performed.

The filter mechanism performs the following functions:

- Inspection - The first 64 bytes of each packet are inspected at full line rate.
- Classification - The classification determines which mask and rule to apply to the packet.
- Trapping - Some packets may be “trapped” to the CPU for further processing. Note that the CPU interface does not operate at line rate.
- Modification - Packets may be modified at wire speed. Modifications to packets are limited to changing the 802.1p priority field and the TOS field in the IP header.
- Port Steering - Packets may be steered to a particular egress port at wire speed.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Mask Table

The Mask table is 8 entries deep and contains the following fields:

Table 12-1: Packet Filtering Mask Table

Field	Width	Description
Egress Port Mask	6 bits	Selects whether the filter is to be applied only on packets destined to certain ports.
Ingress Port Mask	6 bits	Selects whether the filter is to be applied only on packets received on certain ports.
Filter Mask	512 bits (64 bytes)	Selects the bits in the packet that are to be inspected. Note that only up to 32 bytes of the mask may have non-zero values. The remainder of the specified mask must be zero. The underlying hardware is limited to testing up to 32 bytes within the first 64 bytes of the packet.

For all fields in the Mask Table, the value 1 in a bit indicates that the bit is of interest to the mask and a value of 0 indicates that the bit is a ‘Don’t Care.’

Egress Mask

If the user wishes to apply the classification and action to packets destined to a particular port(s), then the Egress Mask field must be set. If this field is set, then the destination port number is “anded” with the value of this field, and the result is compared with the Egress port fields in the Rules Table.

Ingress Mask

If the user wishes to apply the classification and action to packets received on a particular port(s), then the Ingress Mask field must be set. If this field is set, then the ingress port number is “anded” with the value of this field, and the result is compared with the Ingress port fields in the Rules Table.

Filter Mask

This field selects the bits that are of interest to the filter. Any sequence of 1’s and 0’s is valid. The first 512 bits of the packet are effectively “anded” with the value of this field and then compared to Filter fields in the Rules Table.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Rules Table

The Rules table is 126 entries deep, and contains the following fields:

Table 12-2: Packet Filtering Rules Table

Field	Width	Description
Priority	3 bits	Defines the 802.1p priority value to be inserted into the Tag if the Action Field includes Bit 0.
Port	6 bits	Defines the Egress port to be selected (for packet steering) if the Action Field includes Bit 5.[1]
TOS_P	4 bits	Defines the Type Of Service Precedence that is to replace the TOS precedence field in the packet if the Action Field includes Bit 2.
Mask Index	4 bits	Selects the Mask Table entry for which this rule applies.
Ingress Port	6 bits	This field is compared to the result of “and-ing” the Ingress Port Number with the Mask Entry’s Ingress Port Mask value. The result is used to (partially) determine if this rule applies to the packet. Set this to 0 if the Ingress Port is a “Don’t Care” in determining a match.
Egress Port	6 bits	This field is compared to the result of “and-ing” the Egress Port Number with the Mask Entry’s Egress Port Mask value. The result is used to (partially) determine if this rule applies to the packet. Set this to 0 if the Egress Port is a “Don’t Care” in determining a match.
Action	7 bits	Defines the Action to be performed when there is a packet match. The bits are defined in Table 12-3: “Packet Filtering Action Bits”.
Filter	512 bits (64 bytes)	This field is compared to the result of “and-ing” the first 512 bits of the packet with the Mask Entry’s Filter Mask value. The result is used to (partially) determine if this rule applies to the packet. Set this to 0 if the Packet content is a “Don’t Care” in determining a match.

1. The port steering mechanism only works on Unicast packets that have an existing entry in the Filtering Database. Packets to MAC Addresses that are unknown, Multicasts, and Packets destined to any of the switch’s MAC Addresses are not included.

Table 12-3: Packet Filtering Action Bits

Bit Number	Action
0	Select the 802.1p priority from the Priority field in the Rules Entry. The Class of Service Queue (0 - 7) is selected based on the new 802.1p priority field.
1	Select the Class of Service Queue (one of 4) based on the Priority field in the Rules Entry, but leave the 802.1p Priority in the frame unchanged.
2	Change the TOS precedence field in the IP header to the value specified in the TOS_P Field in the Rules Entry.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 12-3: Packet Filtering Action Bits

Bit Number	Action
3	Send a copy of the packet to the CPU.
4	Discard the packet.
5	Select the output port from the Port field in the Rule Entry.
6	Send the packet to the port specified in the mirror-to port. This port is specified via the “mirror to” CLI command. Mirror mode must be enabled.

Matching

Matching is performed in hardware that “ands” the ingress port number, the egress port number, and the first 512 bits of received packets with each mask and then searches the rules associated with each mask for an ingress port, egress port, and filter value that exactly matches the result. This logic can be simply stated as follows:

A rule is matched under the condition that the *Input* “anded” with the *Mask* is equal to the *Rule*, where:

- *Input* = concatenation of (Input Port, Output Port, First 512 bits of Packet)
- *Mask* = concatenation of (Mask.Ingress, Mask.Egress, Mask.Filter)
- *Rule* = concatenation of (Rule.Ingress, Rule.Egress, Rule.Filter)

Match = ((Input & Mask) == Rule)

Using Egress and Ingress Port Masks

Filtering can be done independently of Ingress or Egress port, or it can be done based on a specific Ingress and/or Egress port. Specific Egress port matching can only be done, however, if the destination of a packet can be determined to be a single port. This will only be the case for Unicast packets whose Destination MAC Address is currently in the Filtering Database. Egress port matching cannot be performed for Multicast, Broadcast. or Unknown Destination MAC Addresses.

- If the filtering behavior is not specific to a port, the Mask and Rule entries for ingress and egress ports should be set to 0.
- If filtering is desired for a specific port, the field in the Mask should be set to all 1’s (Decimal 63), and the Rule should contain the desired port number.

Multiple Action Execution and Conflict Resolution

The Masks and Rules are typically configured such that there is only one rule that would apply to each frame for the given mask. If the user does not enforce this, or if multiple mask/rules combinations provide matches, then the conflict resolution algorithm described here applies.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Each Mask should match only a single Rule. The software ensures that each only one Rule with a specific set of match values (Ingress/Egress/Filter) and Mask table index can be added at a time. An error is returned if the user attempts to install multiple rules that all have the same Mask Index, Ingress Port, Egress Port, and Filter values, but with different Action values, or the same Action but differing Priority, Port, or TOS_P values.

Each Rule may execute multiple actions, or a packet may match multiple mask/rule combinations. This is not the same condition described in the previous paragraph. More than one Mask can apply to a packet, and the Actions of the matching Rule from each may be applied (but only one Action from each Mask, as described above).

All non-conflicting actions are executed. If multiple Masks contribute the same Action, then the action is performed only once on a given packet. If a single action, or multiple actions from separate matches, dictates that a packet be given a particular priority *and* be forwarded to the CPU, then both will occur.

When there is a conflict between actions identified through multiple Masks, the action of the higher numbered Mask is executed. For example, if Mask 2 matches a Rule with the action to change the 802.1Q Priority of a frame, but Mask 5 matches a rule with the action to leave the Priority field alone, then the Priority field will be left alone. If these masks were reversed, the Priority field would be changed. This implies that the user should ensure that when conflicting Mask/Rule combinations are intentionally configured, the higher priority Masks have higher index values.

In the event that a single Mask or Rule is incorrectly programmed with conflicting actions, there is an action hierarchy that is followed to resolve the conflict deterministically.

- If the conflict is between changing the 802.1p priority field or leaving it alone, changing the 802.1p priority field takes precedence.

Management Interfaces

Packet Filters are managed through the CLI or through SNMP. There is currently no HTTP Web support. See “Filter Mask Commands” on page 110 for the CLI commands that support Packet Filtering. SNMP support is provided through the Performance Technologies Enterprise MIB under the CPC441xInclusiveFilterMaskTable.

Note: *Packet Filter configurations are not saved in the switch* ***durable*** *file and are not restored upon boot. The user must re-instantiate any User Defined Packet Filters through the use of CLI or Lua scripts invoked by* ***rc.lua****. See “Lua Programming Language” on page 449 and “File System” on page 425.*

Filter Examples

In the following examples, all filters are designed to operate on Tagged Ethernet II Packets using the IP Protocol (without options) and TCP. Viewing the first 64 bytes of these packets as follows, Table 12-4: “Packet Key” on page 317 identifies the various fields:

```
AA AA AA AA AA AA BB BB BB BB BB BB CC CC CC CC
DD DD EE FF GG GG HH HH II II JJ KK LL LL MM MM
MM MM NN NN NN NN OO OO PP PP QQ QQ QQ QQ RR RR
RR RR ST UU VV VV XX XX XX XX XX XX XX XX XX XX
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 12-4: Packet Key

Key Field	Bit Positions
A - MAC Destination Address	1-48
B - MAC Source Address	49-96
C - VLAN Tag (includes priority)	97-128
D - Type	129-144
E - IP Version	145-152
F - TOS	153-160
G - Packet Length	161-176
H - ID Number	177-192
I - Flags	193-208
J - Time To Live (TTL)	209-216
K - Protocol (6 = TCP, 17 = UDP)	217-224
L - IP Checksum	225-240
M - Source IP Address	241-272
N - Destination IP Address	273-304
O - TCP Source Port	305-320
P - TCP Destination Port	321-336
Q - Sequence Number	337-368
R- Acknowledgment Number	369-400
S - Header Length	401-408
T - Reserved	409-412
U- Reserved + Flags	413-416
V - Window Size	417-432
X - other	433-511

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Example 1: Give priority to HTTP traffic and send a copy to the “Mirrored-To” port

This example illustrates how to set up a filter to assign a high priority to HTTP traffic and to forward a copy of this traffic to the Mirrored-To port. This may be used to provide analysis and logging of this type of traffic. The following steps will achieve this:

1. Set Filter Mask on Protocol field in Mac header to FF FFH and the corresponding Filter Value field to 08 00H (IP)
2. Set Filter Mask on Protocol field in IP header to FFH and the corresponding Filter Value field to 06H (TCP).
3. Set Filter Mask on Destination Port number field in TCP header to FF FFH and the corresponding Filter Value field to 00 50H
4. (HTTP = 80 decimal).
5. Set Filter Priority value to 7.
6. Set Filter Mask Index to 2.
7. Set Filter Action to take as 41H, indicating “change 802.1p Priority” AND “send a copy to ‘Mirrored-To’ port”.

Be sure to set the “mirror to” port and enable mirroring (see “Network Diagnostics” on page 175).

Table 12-5: “Packet Filtering Example 1: Mask Entry” illustrates the settings for the Mask Entry for this example:

Table 12-5: Packet Filtering Example 1: Mask Entry

Field	Value
Egress Port Mask	00
Ingress Port Mask	00
Filter Mask	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Table 12-6: “Packet Filtering Example 1: Rule Entry” illustrates the settings for the Rule Entry for this example:

Table 12-6: Packet Filtering Example 1: Rule Entry

Field	Value
Priority	7
Port	00
TOS_P	0
Action	65 (0x41)
Mask Index	2

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 12-6: Packet Filtering Example 1: Rule Entry *(Continued)*

Field	Value
Ingress Port	00
Egress Port	00
Filter	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

The CLI commands to create this filter are:

```
# filter mask add 2 0 0 129-144=f 217-224=f 321-336=f
```

Synopsis:

```
filter mask add <index> <ingress> <egress> <filter...>
# filter rule add 1 7 0 0 0 0 65 2 “mirror http” 129-144=0800 217-224=06
321-336=0050
```

Synopsis:

```
filter rule add <index> <priority> <port> <precedence>  <ingress>
<egress> <action> <mask> <description> <filter...>
```

In addition to setting the packet filter, you also need to establish the mirror-to port and enable mirroring. Use the `mirror to` and the `mirror mode` commands. Normal port mirroring can be used simultaneously with packet mirroring by enabling ingress and/or egress ports. If port mirroring is not desired when using packet mirroring, then disable all ingress and egress port mirrors with the commands `mirror ingress all off` and `mirror egress all off`.

Example 2: Identify SYN and FIN in TCP header and send the packet to a specific port

This example illustrates how to set up a filter to identify SYN and FIN TCP packets and to forward this traffic to the port identified in the Rules entry. This may be used to support detection of socket setup and tear-down, and to allow a device located on the specified port to then verify that the connection should or should not be allowed.

The following steps will achieve this:

1. Set Filter Mask on Protocol field in Mac header to FF FFH and the corresponding Filter Value field to 08 00H.
2. Set Filter Mask on Protocol field in IP header to FFH and the corresponding Filter Value field to 06H.
3. Set Filter Mask on SYN and FIN fields in TCP header to 11b and the corresponding Filter Value field to 11b.
4. Set Filter Mask Index to 3.
5. Set Filter Action to take as 20H, indicating “send the packet to port specified in the Rules Entry”.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 12-7: “Packet Filtering Example 2: Mask Entry” illustrates the settings for the Mask Entry for this example:

Table 12-7: Packet Filtering Example 2: Mask Entry

Field	Value
Egress Port Mask	00
Ingress Port Mask	00
Filter Mask	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00

Table 12-8: “Packet Filtering Example 2: Rule Entry” illustrates the settings for the Rule Entry for this example:

Table 12-8: Packet Filtering Example 2: Rule Entry

Field	Value
Priority	0
Port	8
TOS_P	0
Action	32 (0x20)
Mask Index	3
Ingress Port	00
Egress Port	00
Filter	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00

The CLI commands to create this filter are:

```
# filter mask add 3 0 0 129-144=f 217-224=f 413-416=3
```

Synopsis:

```
filter mask add <index> <ingress> <egress> <filter...>
# filter rule add 2 0 8 0 0 0 32 3 “mirror syn/fin” 129-144=0800 217-
224=06 413-416=3
```

Synopsis:

```
filter rule add <index> <priority> <port> <precedence>  <ingress>
<egress> <action> <mask> <description> <filter...>
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Example 3: Forward all the HTTP traffic coming from port 1 to “Mirrored-To” port

This example illustrates how to set up a filter to forward HTTP traffic on Port 1 to the “Mirrored-To” port for analysis. The following steps will achieve this:

1. Set Filter Mask on Protocol field in Mac header to FF FFH and the corresponding Filter Value field to 08 00H.
2. Set Filter Mask on Protocol field in IP header to FFH and the corresponding Filter Value field to 06H.
3. Set Filter Mask on Destination Port number field in TCP header to FF FFH and the corresponding Filter Value field to 00 50H.
4. Set Filter Mask Index to 4.
5. Set Filter Action to take as 40H, indicating “send packet to Mirrored-to-port.”

Table 12-9: “Packet Filtering Example 3: Mask Entry” illustrates the settings for the Mask Entry for this example:

Table 12-9: Packet Filtering Example 3: Mask Entry

Field	Value
Egress Port Mask	00
Ingress Port Mask	63 (0x3F)
Filter Mask	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Table 12-10: “Packet Filtering Example 3: Rule Entry” illustrates the settings for the Rule Entry for this example:

Table 12-10: Packet Filtering Example 3: Rule Entry

Field	Value
Priority	0
Port	00
TOS_P	0
Action	64 (0x40)
Mask Index	4
Ingress Port	01
Egress Port	00
Filter	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

The CLI commands to create this filter are:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
# filter mask add 4 63 0 129-144=f 217-224=f 321-336=f
```

Synopsis:

```
filter mask add <index> <ingress> <egress> <filter...>
# filter rule add 3 0 0 0 1 0 64 4 “mirror http on 1” 129-144=0800 217-224=06 321-336=0050
```

Synopsis:

```
filter rule add <index> <priority> <port> <precedence> <ingress> <egress> <action> <mask> <description> <filter...>
```

In addition to setting the packet filter, you also need to establish the mirror-to port and enable mirroring. To do this, use the `mirror to` and the `mirror mode` commands. Normal port mirroring can be used simultaneously with packet mirroring by enabling ingress and/or egress ports. If port mirroring is not desired when using packet mirroring, then disable all ingress and egress port mirrors with the commands `mirror ingress all off` and `mirror egress all off`.

Example 4: Change TOS field for Telnet traffic

This example illustrates how to set up a filter to change the TOS field for Telnet Traffic to a specified value. This may be used to adjust the quality of service subsequently provided for Telnet traffic. The following steps will achieve this:

1. Set Filter Mask on Protocol field in Mac header to FF FFH and the corresponding Filter Value field to 08 00H.
2. Set Filter Mask on Protocol field in IP header to FFH and the corresponding Filter Value field to 06H.
3. Set Filter Mask on Destination Port number field in TCP header to FF FFH and the corresponding filter Value field to 00 17H.
4. Set Filter TOS value to 2.
5. Set Filter Mask Index to 5.
6. Set Filter Action to take as 04H, indicating “change Precedence field in IP header”.

Table 12-11: “Packet Filtering Example 4: Mask Entry” illustrates the settings for the Mask Entry for this example:

Table 12-11: Packet Filtering Example 4: Mask Entry

Field	Value
Egress Port Mask	`00`
Ingress Port Mask	`00`

Filter Mask	`00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`
	`FF FF 00 00 00 00 00 00 00 00 FF 00 00 00 00`
	`00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00`
	`00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 12-12: “Packet Filtering Example 4: Rule Entry” illustrates the settings for the Rule Entry for this example:

Table 12-12: Packet Filtering Example 4: Rule Entry

Field	Value
Priority	0
Port	00
TOS_P	2
Action	04
Mask Index	5
Ingress Port	00
Egress Port	00
Filter	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

CLI commands to effect this filter are:

```
# filter mask add 5 0 0 129-144=f 217-224=f 321-336=f
```

Synopsis:

```
filter mask add <index> <ingress> <egress> <filter...>
# filter rule add 4 0 0 2 0 0 4 5 “telnet tos” 129-144=0800 217-224=06
321-336=0017
```

Synopsis:

```
filter rule add <index> <priority> <port> <precedence> <ingress>
<egress> <action> <mask> <description> <filter...>
```

Example 5: Partial BPDU Filter

If BPDU frames are filtered with the ‘filter bpdu’ command (see “Enable or Disable BPDU Filters” on page 113), the user may add a Packet Filter to allow a subset of the Bridge Reserved MAC Addresses to be passed to the CPU. In this example, a Packet Filter is created to detect frames destined to the Spanning Tree BPDU Address and have these passed to the CPU. This allows the switch to discard packets destined to the Reserved Addresses on one or more ports, but still allow those ports to participate in the Spanning Tree protocol.

This example will create a filter that looks at the Destination MAC Address and if the address is 01:80:C2:00:00:00, the packet is passed to the CPU. This filter will not match the MAC Address used for other Bridge protocols including; GMRP (01:80:C2:00:00:20), GVRP (01:80:C2:00:00:21), and LAG (01:80:C2:00:00:02).

Assuming that the user wishes to reject GVRP, GMRP, and LAG on ports 1-8, but allow STP on these ports, the following commands could be used:

```
# filter bpdu 1-8 on
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
# filter mask add 1 0 0 1-48=f
# filter rule add 1 0 0 0 0 0 8 1 "pass stp" 1-48=0180c2000000
```

This mechanism can be tailored to meet other requirements, such as including specific ingress ports to reject all BPDUs on some ports, and allow only STP on some others.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

13

Routing Protocols and IP Multihoming

Overview

This section provides an overview of routing as implemented on the CPC441x. It also describes IP Multihoming, and the two routing protocols supported by the CPC441x: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). The key topics in this chapter include:

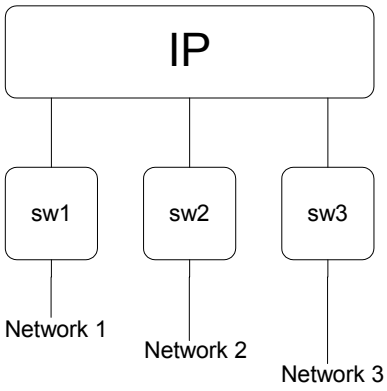
- "Routing (Layer3 Switching)" on page 325
- "Configuring Routing" on page 326
- "IP Multihoming" on page 331
- "RIP (Routing Information Protocol)" on page 334
- "OSPF (Open Shortest Path First)" on page 337

Routing (Layer3 Switching)

Routing directs data between networks. It takes place at Layer3 of the OSI Reference Model, the Network Layer. In order for routing to occur, the user must configure network interfaces for each network connected to a router (see Figure 13-1: "IP Router" on page 326), and enable IP forwarding.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-1: IP Router



Routing Table

A router uses a Routing Table to determine which network interface to use to reach a particular destination. There are three types of Routing Table entries:

- Entries created automatically when network interfaces are configured. Such entries describe directly attached networks.
- Entries added manually by a user. These are referred to as static routes.
- Entries created dynamically by routing protocols such as RIP and OSPF. These are “dynamic” because they are added or removed without the user’s intervention.

MAC Header Rewrite

Unlike Layer2 switches, routers modify packets as they route them from one network to another. This modification, called a “MAC header rewrite,” affects the source and destination MAC addresses, Time To Live (TTL) and the IP header checksum.

VLANs

VLANs group ports into broadcast domains. All internal traffic within a VLAN domain is Layer2-switched, while all inter-VLAN traffic must be routed. When configuring a switch for Layer3, treat sub-networks and VLANs the same.

Configuring Routing

There are four basic steps to configuring routing on the CPC441x:

1. Set VLANs (see Chapter 10, “VLANs,” on page 303).
2. Configure “sw” network interfaces.
3. Enable IP forwarding using the “ip forward” command.
4. Install static routes or enable routing protocols, if applicable.

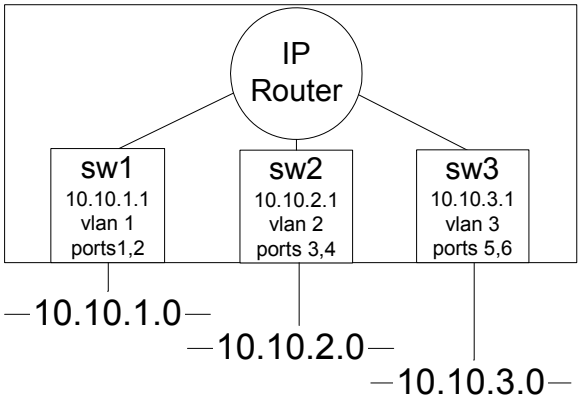
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Example

Our example partitions a network into three sub-networks: 10.10.1.0, 10.10.2.0 and 10.10.3.0, with subnet mask 255.255.255.0. Each subnet will be associated with a different VLAN. To begin, we will create three VLANs and assign ports to each. Then we will create sw network interfaces and assign them to the VLANs, such that:

- sw1 has an IP address 10.10.1.1 and is assigned to VLAN 1
- sw2 has an IP address 10.10.2.1 and is assigned to VLAN 2
- sw3 has an IP address 10.10.3.1 and is assigned to VLAN 3

Figure 13-2: Sub-Networks with VLANs



As a function of the switch architecture each sw interface is connected to an Aggregator (ag), which in turn is connected to an Aggregation Port (ap). The aggregators (ags) are referred to as “logical” ports. (See Chapter 16, “Link Aggregation,” on page 385 for a description of the relationship between physical and logical ports.) We will assume in our example that each ap is attached to its corresponding ag. Throughout this section, logical ports will be referred to as “ports.”

To assign a group of ports to an sw interface, we need to group them into VLANs. The following commands will remove ports 3 - 6 from the default VLAN 1, and create VLAN 2 with ports 3 and 4, and VLAN 3 with ports 5 and 6:

```
#  vlan remove 1 untagged=3-6
#  vlan create 2 vlan2 untagged=3-4
#  vlan create 3 vlan3 untagged=5-6
```

Next, we will create three network interfaces -- sw1, sw2 and sw3 -- and assign them to VLANs 1, 2 and 3, respectively.

```
#  ip config sw1 10.10.1.1 255.255.255.0 1
#  ip config sw2 10.10.2.1 255.255.255.0 2
#  ip config sw3 10.10.3.1 255.255.255.0 3
```

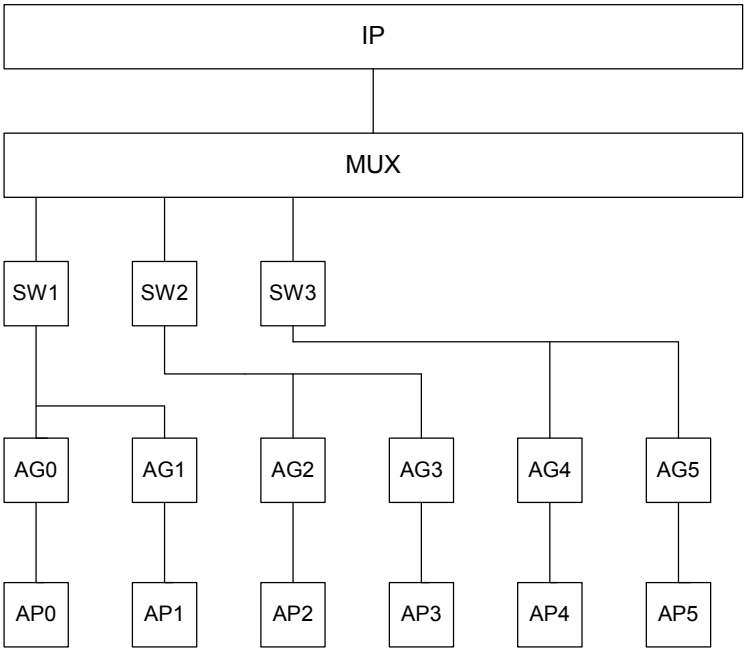
Finally, we will enable IP forwarding and save our configuration:

```
#  ip forward on
#  save
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-3: “Routing Configuration” depicts this configuration:

Figure 13-3: Routing Configuration



To verify that our interfaces are configured correctly, we use the “route show” command to display the Routing Table:

```
#  route show

Destination  Subnet Mask      Next Hop   Description  UseHW S
-------------------------------------------------------------
10.10.1.0    255.255.255.0    10.10.1.1  local        on
10.10.2.0    255.255.255.0    10.10.2.1  local        on
10.10.3.0    255.255.255.0    10.10.3.1  local        on
127.0.0.1    255.255.255.255  127.0.0.1  local        off
S = Static Entry
```

“local” in the Description column indicates that the destination subnet is directly attached and is accessed by a local network interface identified by the Next Hop IP address. “on” in the UseHW column indicates that routing will be done in hardware.

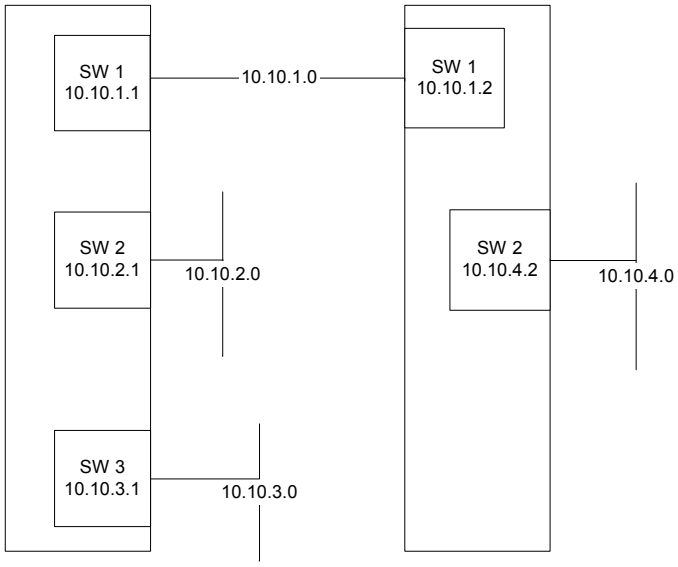
If we add another subnetwork, 10.10.4.0, on a vlan on another switch to which there is a connection, then our routing table does not contain enough information to route traffic to it. There are two ways to correct this:

- Enable a routing protocol, such as RIP (“RIP (Routing Information Protocol)” on page 334) or OSPF (“OSPF (Open Shortest Path First)” on page 337).
- Create a static entry in our routing table.

In our example, network 10.10.4.0 is accessible through another router connected to our switch on network 10.10.1.0, as shown in Figure 13-4: “Network 10.10.4.0”:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-4: Network 10.10.4.0



We can add a static route to network 10.10.4.0 with the following command:

```
#  route add 10.10.4.0 255.255.255.0 10.10.1.2 static on
```

We can verify our settings using the “route show” command:

```
#  route show

Destination  Subnet Mask      Next Hop   Description  UseHW  S
-------------------------------------------------------------
10.10.1.0    255.255.255.0    10.10.1.1  local        on
10.10.1.2    255.255.255.255  10.10.1.1  other        off
10.10.2.0    255.255.255.0    10.10.2.1  local        on
10.10.3.0    255.255.255.0    10.10.3.1  local        on
10.10.4.0    255.255.255.0    10.10.1.2  static       on     *
127.0.0.1    255.255.255.255  127.0.0.1  local        off
S = Static Entry
```

If the next hop, 10.10.1.2, provides the only path to other non-adjacent sub-networks, we don’t need to add a static route for each one; we can create a default gateway instead:

```
#  ip gateway 10.10.1.2
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Again, we use “route show” to verify our settings:

```
#  route show

Destination  Subnet Mask      Next Hop   Description   UseHW  S
-----------------------------------------------------------------
default      0.0.0.0          10.10.1.2  Default Route on     *
10.10.1.0    255.255.255.0    10.10.1.1  local         on
10.10.1.2    255.255.255.255  10.10.1.1  other         off
10.10.2.0    255.255.255.0    10.10.2.1  local         on
10.10.3.0    255.255.255.0    10.10.3.1  local         on
10.10.4.0    255.255.255.0    10.10.1.2  static        on     *
127.0.0.1    255.255.255.255  127.0.0.1  local         off
S = Static Entry
```

Notice that we no longer need the static route for 10.10.4.0. Therefore, we will delete it from our routing table.

```
#  route delete 10.10.4.0
#  route show

Destination  Subnet Mask      Next Hop   Description   UseHW  S
-----------------------------------------------------------------
default      0.0.0.0         10.10.1.2   Default Route on     *
10.10.1.0    255.255.255.0   10.10.1.1   local         on
10.10.1.2    255.255.255.255 10.10.1.1   other         off
10.10.2.0    255.255.255.0   10.10.2.1   local         on
10.10.3.0    255.255.255.0   10.10.3.1   local         on
127.0.0.1    255.255.255.255 127.0.0.1   local         off
S = Static Entry
```

Hardware Limitations

The Layer2 and Layer3 switching functions of the CompactPCI/PSB switch are based on silicon that has fixed-size tables for handling the relationships between IP Addresses, MAC Addresses, and Physical ports. These table sizes result in limitations to the number of network interfaces, hosts, and gateways that the switch can support.

The following table outlines the sizes of the hardware tables on the various switch platforms:

Table 13-1: Hardware Tables

Model	Layer2 Table (MAC to Port)	Layer3 Interface Table (Switch IP Table)	Layer3 Host Table (Host IP to MAC)	Layer3 Network Table (Network Address to Next Hop)
CPC440X	8K	32	2K	16
CPC441X	8K	32	2K	16
CPC5400	8K	32	2K	16
CPC660X	16K	512	4K	4K

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The **Layer2 Table** is also called the Filtering Database. This table maintains the relationship between an attached host's MAC address, VLAN ID, and the port on which it resides.

The **Layer3 Interface table** contains the mapping between each of the switch's SW network interfaces and its MAC Address.

The **Layer3 Host Table** contains the mapping between directly attached host IP Addresses and their MAC Address, VLAN ID, and Port.

The **Layer3 Network Table** contains a list of the gateways known by the switch, including the switch's own gateway addresses. Each network interface that is configured on the switch is a potential gateway and therefore consumes an entry in this table. One table entry is also used for each Static or Dynamic Route. Two table entries are used for a Default Gateway. If a network grows beyond the limits imposed by this table, the switch will route in software, which will significantly degrade performance. If this limitation is reached, it is recommended that the user make greater use of static routes rather than routing protocols, or partition the network into several areas and use OSPF (see "OSPF (Open Shortest Path First)" on page 337) rather than RIP (see "RIP (Routing Information Protocol)" on page 334).

IP Multihoming

The term "multihoming" is used to describe both an IP system with multiple network interfaces, and an individual interface with multiple IP addresses. By either definition, the CPC441x is a mutihomed device. The CPC441x can support up to 14 different SW network interfaces. In addition, addresses belonging to the same interface may be in the same or different sub-networks.

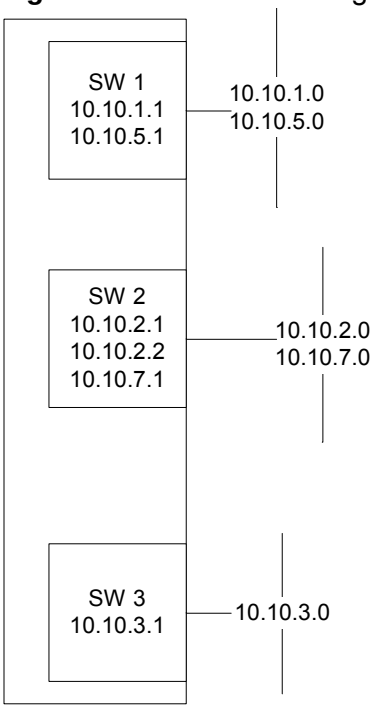
Assigning more than one IP address to a single SW interface is simple and straightforward. Once an interface is created and assigned to a VLAN using the "ip config" command, more addresses can be added to it using the same command. The SW interface can belong to multiple sub-networks, but it can be associated with only one VLAN; assigning a new VLAN ID replaces the previous VLAN association.

We can illustrate setting IP multihoming on sw interfaces in Figure 13-5: "IP Multihoming on SW Interfaces" on page 332. We will create three network interfaces: sw1, sw2 and sw3, such that:

- sw1 will be assigned to VLAN 1 and will have IP addresses: 10.10.1.1 and 10.10.5.1
- sw2 will be assigned to VLAN 2 and will have IP addresses: 10.10.2.1, 10.10.2.2 and 10.10.7.1
- sw3 will be assigned to VLAN 3 and will have IP address: 10.10.3.1

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-5: IP Multihoming on SW Interfaces



First, we use the following commands to remove four ports from the default VLAN 1, and to create VLAN 2 and VLAN 3, with two ports assigned to each:

```
#  vlan remove 1 untagged=3-6
#  vlan create 2 vlan2 untagged=3-4
#  vlan create 3 vlan3 untagged=5-6
```

Next, we will create three network interfaces: sw1, sw2 and sw3:

```
#  ip config sw1 10.10.1.1 255.255.255.0 1
#  ip config sw1 10.10.5.1
#  ip config sw2 10.10.2.1 255.255.255.0 2
#  ip config sw2 10.10.2.2
#  ip config sw2 10.10.7.1
#  ip config sw3 10.10.3.1 255.255.255.0 3
```

Notice that if no mask or VLAN ID is provided, the existing mask and VLAN ID is assumed.

Finally, we will enable IP forwarding and save our configuration into NVRAM:

```
#  ip forward on
#  save
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

We can verify our settings using the “ip stats sw” command:

```
#  ip stats sw

Interface  : sw1
Name       : None
Status     : Active
MAC        : 00:c0:8c:e8:95:5e
VID        : 1
IP address : 10.10.1.1
Netmask    : 255.255.255.0
IP address : 10.10.5.1
Netmask    : 255.255.255.0

Interface  : sw2
Name       : None
Status     : Active
MAC        : 00:c0:8c:e8:95:de
VID        : 2
IP address : 10.10.2.1
Netmask    : 255.255.255.0
IP address : 10.10.2.2
Netmask    : 255.255.255.0
IP address : 10.10.7.1
Netmask    : 255.255.255.0

Interface  : sw3
Name       : None
Status     : Active
MAC        : 00:c0:8c:e8:95:3e
VID        : 3
IP address : 10.10.3.1
Netmask : 255.255.255.0
```

We can also examine the new routing table:

```
#  route show

Destination  Subnet Mask      Next Hop   Description   UseHW  S
-----------------------------------------------------------------
default      0.0.0.0          10.10.1.2  Default Route on     *
10.10.1.0    255.255.255.0    10.10.1.1  local         on
10.10.1.2    255.255.255.255  10.10.1.1  other         off
10.10.2.0    255.255.255.0    10.10.2.1  local         on
10.10.3.0    255.255.255.0    10.10.3.1  local         on
10.10.5.0    255.255.255.0    10.10.5.1  local         on
10.10.7.0    255.255.255.0    10.10.7.1  local         on
127.0.0.1    255.255.255.255  127.0.0.1  local         off
S = Static Entry
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

RIP (Routing Information Protocol)

Routing Information Protocol (RIP) is a distance-vector protocol that uses hop count as its metric. RIP is widely used for routing traffic and is an *interior gateway protocol* (IGP), which means that it performs routing within a single autonomous system. Exterior gateway protocols, such as the Border Gateway Protocol (BGP), perform routing between different autonomous systems. The latest enhancement to RIP is the RIP 2 specification, which allows more information to be included in RIP packets and provides a simple authentication mechanism. The CPC441x supports both RIP and RIP2.

Note: *RIP and OSPF include the management port as a route interface. When these protocols are enabled, the user may wish to specifically disable them on the management port to prevent the switch from advertising routes to the switch interface via the management port. The commands to disable RIP and OSPF on the management port are "route rip disable <ip>" and "route ospf interface admin <interface> off".*

IP RIP is formally defined in two documents: Request For Comments (RFC) 1058 and 1723. RFC 1058 (1988) describes the first implementation of RIP, while RFC 1723 (1994) updates RFC 1058. RFC 1058 enables RIP messages to carry more information and security features.

Routing Updates

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by one, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

RIP Routing Metric

RIP uses a single routing metric — hop count — to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop-count value, which is typically 1. When a router receives a routing update that contains a new or changed destination-network entry, the router adds one to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop.

RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by one causes the metric to be infinity (that is, 16), the network destination is considered unreachable.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

RIP Stability Features

To adjust for rapid network-topology changes, RIP specifies a number of stability features that are common to many routing protocols. RIP, for example, implements the split-horizon and hold-down mechanisms to prevent incorrect routing information from being propagated. In addition, the RIP hop-count limit prevents routing loops from continuing indefinitely.

RIP Timers

RIP uses numerous timers to regulate its performance. These include a *routing-update timer*, a *route timeout*, and a *route-flush timer*. The routing-update timer clocks the interval between periodic routing updates. Generally, it is set to 30 seconds, with a small random number of seconds added each time the timer is reset to prevent collisions. Each routing-table entry has a route-timeout timer associated with it. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires.

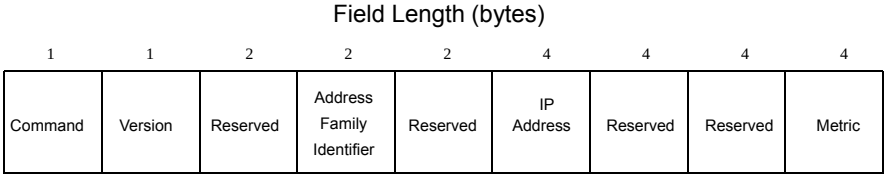
Packet Formats

The following section focuses on the IP RIP and IP RIP 2 packet formats illustrated in Figure 13-6: “RIP Packet” and Figure 13-7: “RIP 2 Packet”. Each illustration is followed by descriptions of the fields.

RIP Packet Format

Figure 13-6: “RIP Packet” illustrates the IP RIP packet format.

Figure 13-6: RIP Packet



The following descriptions summarize the IP RIP packet-format fields illustrated in Figure 13-6: “RIP Packet”:

- *Command*—Indicates whether the packet is a request or a response. The request asks that a router send all or part of its routing table. The response can be an unsolicited regular routing update or a reply to a request. Responses contain routing table entries. Multiple RIP packets are used to convey information from large routing tables.
- *Version Number*—Specifies the RIP version used. This field can signal different potentially incompatible versions.
- *Reserved*—Not used, must be set to zero.
- *Address-Family Identifier (AFI)*—Specifies the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an address-family identifier to indicate the type of address being specified. The AFI for IP is 2.
- *IP Address*—Specifies the IP address for the entry.
- *Metric*—Indicates how many internetwork hops (routers) have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route.

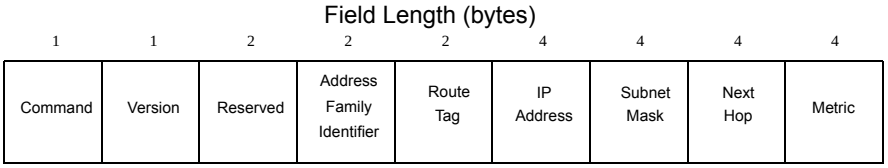
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Note: *Up to 25 occurrences of the AFI, address, and metric fields are permitted in a single IP RIP packet. That is, up to 25 destinations can be listed in a single RIP packet.*

RIP 2 Packet Format

Figure 13-7: “RIP 2 Packet” illustrates the IP RIP 2 packet format.

Figure 13-7: RIP 2 Packet



The RIP 2 specification (described in RFC 1723) allows more information to be included in RIP packets and provides a simple authentication mechanism.

The following descriptions summarize the IP RIP 2 packet format fields.

- *Command*—Indicates whether the packet is a request or a response. The request asks that a router send all or a part of its routing table. The response can be an unsolicited regular routing update or a reply to a request. Responses contain routing-table entries. Multiple RIP packets are used to convey information from large routing tables.
- *Version*—Specifies the RIP version used. In a RIP packet implementing any of the RIP 2 fields or using authentication, this value is set to 2.
- *Reserved*—Value set to zero.
- *Address-Family Identifier (AFI)*—Specifies the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an address-family identifier to indicate the type of address specified. The address-family identifier for IP is 2. If the AFI for the first entry in the message is 0xFFFF, the remainder of the entry contains authentication information. Currently, the only authentication type is simple password.
- *Route Tag*—Provides a method for distinguishing between internal routes (learned by RIP) and external routes (learned from other protocols).
- *IP Address*—Specifies the IP address for the entry.
- *Subnet Mask*—Contains the subnet mask for the entry. If this field is zero, no subnet mask has been specified for the entry.
- *Next Hop*—Indicates the IP address of the next hop to which packets for the entry should be forwarded.
- *Metric*—Indicates how many internetwork hops (routers) have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route.

Note: *Up to 25 occurrences of the AFI, address, and metric fields are permitted in a single IP RIP packet. That is, up to 25 routing table entries can be listed in a single RIP packet. If the AFI specifies an authenticated message, only 24 routing table entries can be specified.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

OSPF (Open Shortest Path First)

OSPF was developed by the Internet Engineering Taskforce (IETF) to provide a high-functionality non-proprietary Internal Gateway Protocol (IGP) for the TCP/IP protocol family. It is a link-state routing protocol that builds a complete picture of a network, unlike the vector-based algorithms used in traditional Internet routing protocols, such as RIP. OSPF supports Classless Interdomain Routing (CIDR), and has introduced concepts such as authentication of routing updates, variable length subnet masks (VLSM), and route summarization. Unlike RIP, OSPF is well suited for large networks. Performance Technologies' OSPFv2 implementation conforms to RFC2328, RFC1850, RFC1587, RFC1765, RFC2370.

Note: *OSPF protocol packets use an IP Type of Service (TOS) of '0'. Table 13-2: "OSPF General Parameters" indicates additional Performance Technologies exceptions to the RFC1850 MIB.*

Table 13-2: OSPF General Parameters

Field	MIB	Object(s)	Syntax	Access	Notes
Router ID	RFC1850	ospfRouterId	RouterID	R-W	
Admin Status	RFC1850	ospfAdminStat	Status	R-W	Implemented as read-only.
Version	RFC1850	ospfVersionNumber	INTEGER	R-O	
Area Border Router	RFC1850	ospfAreaBdrRtrStatus	TruthValue	R-O	
AS Border Router	RFC1850	ospfASBdrRtrSTatus	TruthValue	R-W	
External LSA Count	RFC1850	ospfExternLsaCount	Gauge32	R-O	
External LSA Checksum Sum	RFC1850	ospfExternalLsaCksumSum	Integer32	R-O	
TOS Support	RFC1850	ospfTOSSupport	TruthValue	R-W	Implemented as read-only.
New LSA Received	RFC1850	ospfRxNewLsas	Counter32	R-O	
External LSDB Limit	RFC1850	ospfExtLsdbLimit	Integer32	R-W	Implemented as read-only.
Exit Overflow Interval	RFC1850	ospfExitOverflowInterval	PositiveInteger	R-W	Implemented as read-only.

OSPF vs. RIP

- RIP has a limit of 15 hops; a RIP network that spans more than 15 hops (15 routers) is considered unreachable. OSPF has no limit on hop count.
- RIP cannot handle Variable Length Subnet Masks (VLSM). Given the shortage of IP addresses and the flexibility VLSM provides in the efficient assignment of IP addresses, this is considered a major flaw. OSPF supports the intelligent use of VLSM.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- OSPF is more complex than RIP and requires more CPU and memory resources, but converges faster than RIP and uses less network resources.
- RIP's periodic broadcasts of the full routing table consume a large amount of bandwidth. OSPF uses IP multicast to send link-state updates, ensuring less processing on routers that are not listening to OSPF packets. Also, updates are sent only in the event of routing changes instead of periodically.
- RIP routers go through a period of hold-down and garbage collection, and slowly time-out information that has not been received recently, resulting in convergence that sometimes takes minutes. This is inappropriate in large environments, and could cause routing inconsistencies. Because OSPF propagates routing changes instantaneously, it converges faster.
- RIP has no concept of network delays and link costs. The path with the lowest hop count to the destination is always preferred even if the longer path has a better aggregate link bandwidth and shorter delays.
- RIP networks are flat, with no concept of areas or boundaries. OSPF allows for the logical definition of networks, where routers can be divided into areas. This reduces the explosion of link-state updates over the entire network. This also provides for aggregating routes and cutting down on the unnecessary propagation of subnet information.

Some enhancements were introduced in a new version of RIP called RIP2, which address the issues of VLSM, authentication, and multicast routing updates. RIP2, however, is not a major improvement over RIP (now called RIP1) because it still has the limitations of hop counts and slow convergence, which are serious shortcomings in today's large networks.

OSPF Concepts

- OSPF is classified as an interior gateway protocol, meaning it is designed to route within a single Autonomous System (AS). It finds the shortest path to a destination based on the algorithm employed.
- OSPF supports two-tier hierarchical topology using the concept of areas, which are contiguous portions of a network within an AS. Each area uses a separate topology database and is invisible to all other areas. The use of OSPF areas minimizes the amount of routing traffic.
- OSPF (unlike RIP) can support more than one metric. When using a single metric, the Type of Service (TOS) is not used. The TOS is optional when using two or more metrics.
- OSPF routes IP packets based on the IP destination address and the IP TOS (Type of Service) information contained in the IP header. Note that OSPF may use different routes to a destination based on the TOS.
- OSPF allows for the transfer and tagging of external routes injected into an Autonomous System. This keeps track of external routes injected by exterior protocols, such as BGP.

OSPF Tables

OSPF maintains three databases: Neighbor Database, Topology Database and Routing Table. The most important of the three is a Routing Table. Routing decisions are based on the information contained in the Routing Table.

Topology Table

OSPF maintains a picture of the entire network in its Topology Table. This database contains information about router relationships and types, links, types of links (router or network), advertising routers, and links contained in particular areas (except for summary links). The complete OSPF database, stored by area, can be viewed with the following command:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
# route ospf show database
```

Routing Table

The Routing Table contains the actual routing entries, which are looked at when packets need to be routed from one subnetwork to another. To view the entire routing table, execute the following command:

```
# route dump
```

Neighbor Table

This database lists the neighbors of this router. It keeps information on each neighbor's router ID, priority, state, dead time, address, and the interface through which this router connects to the neighbor. To view the Neighbor Table, execute this command:

```
# route ospf show neighbor
```

Neighbor Relationships

Routers proceed through a series of states in order to fully implement OSPF, starting as neighbors and finally becoming adjacent.

Becoming a Neighbor

Becoming a neighbor is the first step that a router takes to achieve its eventual goal of building a topology database and routing table. Exchanging hello packets is the method used to become neighbors, a condition which is achieved when the router sees itself listed in a neighbor's hello packet.

Adjacency

Once routers become neighbors, they then continue on in the database exchange state, known in OSPF terminology as becoming adjacent. During this stage, the routers go through several states (INIT, Two-way/Exstart, Two-way/Exchange, Two-way/Loading, FULL) until they have successfully completed their database exchange.

Designated Router (DR) and Backup Designated Router (BDR)

On broadcast networks such as Ethernet, OSPF has mechanisms for reducing the number of adjacencies formed. It does so by electing a designated router (DR) and a backup designated router (BDR). All routers become adjacent with DR and BDR and send their link-state updates (LSUs) to DR and BDR only. It is important to understand that although all OSPF routers on a broadcast network will become neighbors with each other, they will become adjacent only with the DR and the BDR.

The DR is responsible for sending the Link State Advertisements (LSAs) to all other routers on the network. The BDR does not send LSAs, although it does receive all that the DR receives. In the event that the DR fails, the BDR takes over, and a new BDR is elected. All OSPF routers listen on the multicast address 224.0.0.5. Only DR and BDR receive traffic destined to the multicast IP address 224.0.0.6.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The election of the DR and BDR depends on whether all routers are powered up at the same time or not. The first OSPF router up on the network will become a DR. The second router up on the network will become a BDR. If routers are powered up simultaneously, then the router with the highest priority will become a DR and the router with the second highest priority value will become a BDR. The default priority value is 1. Priority zero indicates that the OSPF router cannot become a DR or BDR. If the priorities are equal, then the router ID (the highest IP address of an active interface) will become a tiebreaker. The router with the highest ID will become a DR and the router with the second highest ID will become a BDR.

Link State Advertisements (LSAs)

The Link State Advertisements are not packets but are fields inside other packets, such as Database Description (DD) packets. LSAs summarize the contents of the link-state database of the sending routers. There are five basic LSA types supported by the CPC441x:

- LSA Type 1, Router LSA, is sent by each router in an area for each interface (called link) participating in the OSPF process.
- LSA Type 2, Network LSA, is sent by the DR and describes the state of all routers on the network segment.
- LSA Type 3, Summary LSA, is sent by the Area Border Router (ABR) to the backbone.
- LSA Type 4, Summary LSA, is sent by the Area Border Router (ABR) destined for an Autonomous System Border Router (ASBR).
- LSA Type 5, Autonomous System External LSA, is sent by ASBRs describing particular destinations external to the AS, and is also used to describe a default route.

Opaque LSAs

In addition to the five LSAs described above, the CPC441x also supports “opaque” LSAs (types 9, 10 and 11). Opaque LSAs provide for the future extensibility of OSPF. Opaque LSAs consist of a standard LSA header followed by application-specific information. Standard OSPF link-state database flooding mechanisms are used to distribute opaque LSAs to all or some of the OSPF topology.

- LSA Type 9 denotes a link-local scope. Type 9 opaque LSAs are not flooded beyond the local (sub)network.
- LSA Type 10 denotes an area-local scope. Type 10 LSAs are not flooded beyond the borders of their associated area.
- LSA Type 11 denotes that the LSA is flooded throughout the autonomous system (AS). The flooding scope of type 11 LSAs is equivalent to the flooding scope of AS-external (Type 5) LSAs. Type 11 opaque LSAs are:
  - flooded throughout all transit areas
  - not flooded into stub areas from the backbone
  - not originated by routers into their connected stub areas

  As with Type 5 LSAs, if a Type 11 opaque LSA is received in a stub area from a neighboring router within the stub area, the LSA is rejected.

Opaque LSAs are disabled by default on the CPC441x.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Disabling Opaque LSAs on Cisco Routers

By default, opaque LSAs (types 9, 10, and 11) are disabled on the CPC441x. If the CPC441x is connected to a router which by default enables opaque LSAs, such a a Cisco router, then they will not interoperate unless either:

- opaque LSAs are enabled on the CPC441x, to match the configuration of the other router, or
- opaque LSAs are disabled on the other router, to match the CPC441x configuration.

To enable opaque LSAs on the CPC441x, execute the following command:

```
# route ospf opaque on
```

To disable opaque LSAs on Cisco routers:

1. Login to your Cisco router. You will be prompted to enter a password.
2. Enter privileged configuration mode by typing `enable`. You will be prompted to enter the privileged mode password.
3. Enter a global configuration mode by typing `enable terminal`.
4. Enter the OSPF configuration mode. Because the Cisco router can have more than one OSPF process running, you must include an OSPF process number. For example, if your OSPF process number is 1, then the command to enter the OSPF configuration mode is:

   ```
   router ospf 1
   ```

   You can verify your OSPF process number by executing the `show run` command in the global configuration mode.
5. Disable opaque LSAs by entering the following command:

   ```
   no capability opaque
   ```
6. Exit each of the configuration modes by typing `exit`.

Here is a summary of the commands presented above:

```
enable
# configure terminal
(config)# router ospf 1
(config-router)# no capability opaque
(config-router)# exit
(config)# exit
#
```

OSPF Areas

As the number of routers and networks in your organization grows larger, maintaining them becomes increasingly difficult. OSPF allows breaking a large network into smaller, more manageable areas. As a rule of thumb, there should be no more than 50 routers in one area. All areas must connect to Area 0 which is called the backbone.

Internal Router

Internal routers have all interfaces located within a single area and require only one link-state database.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Area Border Router (ABR)

Area Border Routers (ABRs) have interfaces in non-backbone areas and at least one in the backbone area (area 0). This router summarizes connected areas and advertises the networks to the backbone, where the summary routes are sent to each ABR. The ABR must run a separate copy of the OSPF algorithm for each area to which it is connected.

Backbone Router

A backbone router is a router that has at least one interface connected to area 0. ABRs qualify as backbone routers, but not all backbone routers are ABRs. When all of a router's interfaces are in area 0, then the router is a backbone router but it is not an ABR.

Autonomous System Boundary Router (ASBR)

The autonomous system boundary router (ASBR) redistributes routes learned from other autonomous systems into the OSPF domain. It can also redistribute routes learned from other routing protocols such as RIP, IGRP, EIGRP and BGP. The CPC441x allows only one routing protocol to run at any given time, and therefore it does not allow the redistribution of routes from other protocols. In other words, the CPC441x cannot support the ASBR functionality unless both Autonomous Systems are running OSPF.

OSPF Configuration Examples

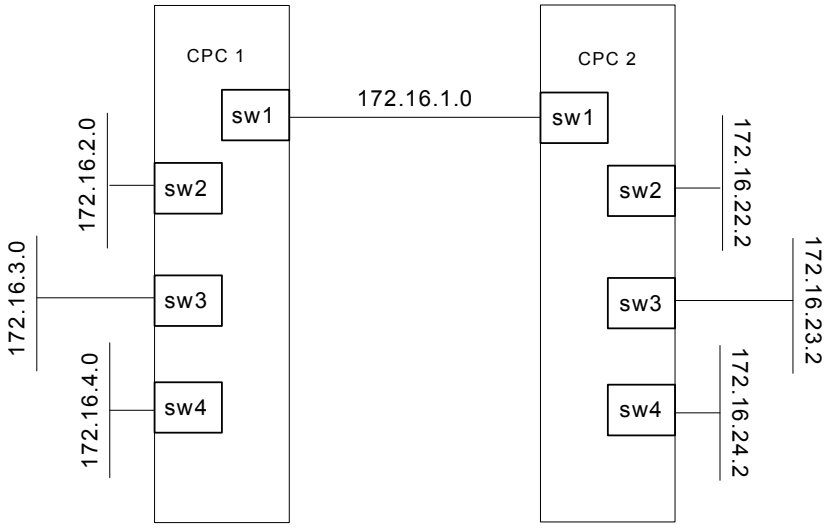
Single Area Configuration Example

In this simple example we will connect two switches (cpc1 and cpc2) to the same network segment (see Figure 13-8: "Single Area Configuration" on page 343). OSPF considers a network such as Ethernet to be a broadcast network. On a broadcast network, OSPF routers will become adjacent (the CPC441x acts as an OSPF router). OSPF will also elect a Designated Router (DR) and a Backup Designated Router (BDR). The network segment that connects the two switches together is 171.16.1.0. where the third byte in the IP address represents a subnetwork (netmask 255.255.255.0). Both switches connect to network 172.16.1.0 via network interface sw1. Both switches also connect to three different subnetworks.

Note: *The examples provided in this section refer to the CPC440x (26 ports), but the implementation of OSPF they illustrate is the same for the CPC441x, CPC54xx, CPC64xx, and CPC660x Ethernet switches.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-8: Single Area Configuration



On cpc1:

- cpc1 connects to cpc2 on subnetwork 172.16.1.0 via sw1 (172.16.1.1)
- sw2 connects to subnetwork 172.16.2.0
- sw3 connects to subnetwork 172.16.3.0
- sw4 connects to subnetwork 172.16.4.0

On cpc2:

- cpc2 connects to cpc1 on subnetwork 172.16.1.0 via sw1 (172.16.1.2)
- sw2 connects to subnetwork 172.16.22.0
- sw3 connects to subnetwork 172.16.23.0
- sw4 connects to subnetwork 172.16.24.0

In order to configure network interface drivers, we first need to create VLANs which represent all four subnetworks. The factory default is such that all ports belong to VLAN 1 (the default VLAN). As we create various VLANs, we also need to remove these ports from the default VLAN.

```
cpc1#  vlan create 2 vlan2 untagged=4-5
cpc1#  vlan create 3 vlan3 untagged=6-8
cpc1#  vlan create 4 vlan4 untagged=9-12
cpc1#  vlan create 5 vlan5 untagged=13-16
cpc1#  vlan remove 1 untagged=4-16
```

The first four commands assigned ports 4-5 to VLAN 2, ports 6-8 to VLAN 3, ports 9-12 to VLAN 4, and ports 13-16 to VLAN 5. The last command removed ports 4-16 from the default VLAN 1.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

To verify that all VLANs are configured correctly, execute the vlan show command:

```
cpc1#  vlan show

VLAN NAME  VLAN ID  12345678901234567890123456
-------------------------------------------
Default    1        UUU-------------UUUUUUUUUU
vlan2      2        ---UU---------------------
vlan3      3        -----UUU-----------------
vlan4      4        --------UUUU--------------
vlan5      5        ------------UUUU----------
```

The following commands configure network interface drivers and assign them to their respective VLANs: sw1 is being assigned to VLAN 2, sw2 is being assigned to VLAN 3, sw3 to VLAN 4, and sw4 to VLAN 5.

```
cpc1#  ip config sw1 172.16.1.1 255.255.255.0 2
cpc1#  ip config sw2 172.16.2.1 255.255.255.0 3
cpc1#  ip config sw3 172.16.3.1 255.255.255.0 4
cpc1#  ip config sw4 172.16.4.1 255.255.255.0 5
```

You can verify that all your network interfaces are configured correctly by examining the routing table. All local network interfaces will show as “local” routing entries.

```
cpc1# route dump

Destination  Subnet Mask      Next Hop    Age  Metr  Protocol
-------------------------------------------------------------
127.0.0.1    255.255.255.255  127.0.0.1   590  0     local
172.16.1.0   255.255.255.0    172.16.1.1  592  0     local
172.16.1.2   255.255.255.255  172.16.1.1  592  0     other
172.16.2.0   255.255.255.0    172.16.2.1  592  0     local
172.16.3.0   255.255.255.0    172.16.3.1  592  0     local
172.16.4.0   255.255.255.0    172.16.4.1  592  0     local
```

Now that all network interfaces have been created, we can enable the OSPF routing protocol on cpc1, but first we must assign an OSPF ID. The following commands assign an OSPF ID and enable OSPF:

```
cpc1#  route ospf id 172.16.1.1
cpc1#  route enable ospf
```

Next, we need to create area 0 (a backbone area). The following command creates area 0 on the cpc1:

```
cpc1#  route ospf area add 0.0.0.0
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The OSPF process will not advertise its network interfaces until they are added to OSPF and assigned to an area. This is done with the “route ospf interface add” command. The following set of commands adds all four network interfaces to area 0:

```
cpc1#  route ospf interface add 172.16.1.1 0.0.0.0
cpc1#  route ospf interface add 172.16.2.1 0.0.0.0
cpc1#  route ospf interface add 172.16.3.1 0.0.0.0
cpc1#  route ospf interface add 172.16.4.1 0.0.0.0
```

Finally, we need to save the configuration to nvram:

```
cpc1#  save
```

To assign network interfaces to different areas, you need to create a new area with the “route ospf area” command, and then associate the new area with the network interface, using the “route ospf interface add” command. Each network interface can be a member of only one area. Therefore, if a network interface has previously been assigned to an area, it must first be removed from that area before being assigned to a different area. To remove a network interface from an area, use the “route ospf interface remove” command:

The configuration for cpc 2 looks like the following:

```
cpc2#  vlan create 2 vlan2 untagged=5-7
cpc2#  vlan create 3 vlan3 untagged=8-10
cpc2#  vlan create 4 vlan4 untagged=11-14
cpc2#  vlan create 5 vlan5 untagged=15-20
cpc2#  vlan remove 1 untagged=5-20
```

Again, you can verify that your VLAN configuration is correct by using the `vlan show` command:

```
cpc2#  vlan show

VLAN NAME  VLAN ID  123456789012345678901234567890123456
Default    1        UUUU----------------UUUUUU
vlan2      2        ----UUU-------------------
vlan3      3        -------UUU----------------
vlan4      4        ----------UUUU------------
vlan5      5        --------------UUUUUU------
```

Next, you need to configure sw network interfaces:

```
cpc2#  ip config sw1 172.16.1.2 255.255.255.0 2
cpc2#  ip config sw2 172.16.22.2 255.255.255.0 3
cpc2#  ip config sw3 172.16.23.2 255.255.255.0 4
cpc2#  ip config sw4 172.16.24.2 255.255.255.0 5
```

When all network interfaces are created, we can configure OSPF:

```
cpc2#  route ospf id 172.16.1.2
cpc2#  route enable ospf
cpc2#  route ospf area add 0.0.0.0
cpc2#  route ospf interface add 172.16.1.2 0.0.0.0
cpc2#  route ospf interface add 172.16.22.2 0.0.0.0
cpc2#  route ospf interface add 172.16.23.2 0.0.0.0
cpc2#  route ospf interface add 172.16.24.2 0.0.0.0
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
cpc2#  save
```

To view the neighbor database on cpc1, execute the following command:

```
cpc1#  route ospf show neighbor
```

This produces the following display:

```
IP Address  Router ID   Optns  Pri  State  Evnt  Dynamic
-------------------------------------------------------
172.16.1.2  172.16.1.2  2      1    full   5159  on
```

The IP address is the address of the (sw) Network Interface of the neighbor router. Router ID is the IP address assigned to the neighbor router as its Router ID. Priority 1 means that the neighbor router is capable of becoming a DR or a BDR. Remember that any router with a priority of “0” cannot become a DR or a BDR. State “full” indicates that our router (cpc1) has established “full” adjacency with cpc2.

Executing the same `show neighbor` command on cpc2 will produce the following:

```
IP Address  Router ID   Optns  Pri  State  Evnt  Dynamic
-------------------------------------------------------
172.16.1.1  172.16.1.1  2      1    full   5159  on
```

We can also examine the routing table on both routers to see whether cpc1 and cpc2 have learned any routes from OSPF:

```
cpc1#  route dump
```

This command will produce the following display:

```
Destination  Subnet Mask      Next Hop    Age  Metr  Protocol
-------------------------------------------------------------
127.0.0.1    255.255.255.255  127.0.0.1   590  0     local
172.16.1.0   255.255.255.0    172.16.1.1  592  0     local
172.16.1.2   255.255.255.255  172.16.1.1  592  0     other
172.16.2.0   255.255.255.0    172.16.2.1  592  0     local
172.16.3.0   255.255.255.0    172.16.3.1  592  0     local
172.16.4.0   255.255.255.0    172.16.4.1  592  0     local
172.16.22.0  255.255.255.0    172.16.1.2  589  1     ospf
172.16.23.0  255.255.255.0    172.16.1.2  589  1     ospf
172.16.24.0  255.255.255.0    172.16.1.2  589  1     ospf
```

Notice that the last three routes were learned by OSPF. Also notice that the OSPF routes have a different metric than the local routes. All local routes have a metric of “0,” the lowest metric. The OSPF routes, on the other hand, will have a metric that is related to the speed of the link.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

You may also examine the Link State Advertisements (LSAs) by displaying the OSPF database:

```
cpc1#  route ospf show database

Router Link Status

Area     Link ID     Router ID   Age  Sequence      Chksum
-------------------------------------------------------------
0.0.0.0  172.16.1.1  172.16.1.1  873  0x0800000a9   0x122b
0.0.0.0  172.16.1.2  172.16.1.2  848  0x080000087   0x1808

Net Link States

Area     Link ID     Router ID   Age  Sequence      Chksum
-------------------------------------------------------------
0.0.0.0  172.16.1.1  172.16.1.1  904  0x0800000a8   0x991d
0.0.0.0  172.16.2.1  172.16.1.1  9022 0x0800000a5   0x3745
0.0.0.0  172.16.3.1  172.16.1.1  923  0x0800000a6   0x2a50
0.0.0.0  172.16.4.1  172.16.1.1  923  0x0800000a7   0x1d5b
0.0.0.0  172.16.22.2 172.16.1.2  879  0x080000084   0x96ef
0.0.0.0  172.16.23.2 172.16.1.2  879  0x080000085   0x89ef
0.0.0.0  172.16.24.2 172.16.1.2  879  0x080000086   0x7c06
```

Finally, you can examine the network interfaces participating in the OSPF process by executing the following command.

```
cpc1#  route ospf interface show

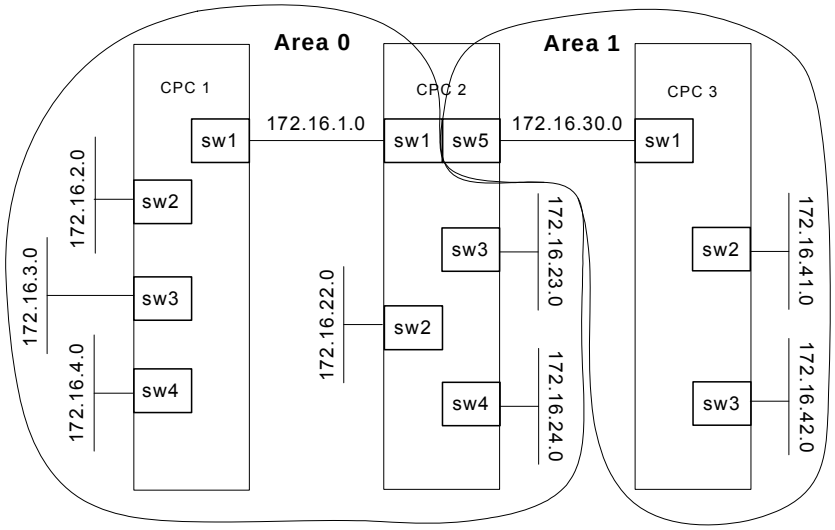
Iface    IP          Area     State              Admin State
-------------------------------------------------------------
sw1      172.16.1.1  0.0.0.0  designated router  on
sw2      172.16.2.1  0.0.0.0  designated router  on
sw3      172.16.3.1  0.0.0.0  designated router  on
sw4      172.16.4.1  0.0.0.0  designated router  on
```

Multiple Area Configuration Examples

In this example we will create two areas: area 0 and area 1, see Figure 13-8: “Single Area Configuration”. To accomplish this, we will use three switches: cpc1, cpc2 and cpc3. Cpc1 and cpc2 will have network interfaces in area 0. We will configure cpc2 as an Area Border Router by placing one of its interfaces in area 1. Cpc3 will have all its network interfaces in area 1.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-9: Multiple Area Configuration



The three switches will be configured as follows:

Area 0

- cpc1 connects to cpc2 on subnetwork 172.16.1.0 via sw1 (172.16.1.1)
- On cpc1 sw2 connects to subnetwork 172.16.2.0
- On cpc1 sw3 connects to subnetwork 172.16.3.0
- On cpc1 sw4 connects to subnetwork 172.16.4.0
- cpc2 connects to cpc1 on subnetwork 172.16.1.0 via sw1 (172.16.1.2)
- On cpc2 sw2 connects to subnetwork 172.16.22.0
- On cpc2 sw3 connects to subnetwork 172.16.23.0
- On cpc2 sw4 connects to subnetwork 172.16.24.0

Area 1

- cpc2 connects to cpc3 on subnetwork 172.16.30.0 via sw5 (172.16.30.2)
- cpc3 connects to cpc2 on subnetwork 172.16.30.0 via sw1 (172.16.30.3)
- On cpc3 sw2 connects to subnetwork 172.16.41.0
- On cpc3 sw3 connects to subnetwork 172.16.42.0

The configuration for cpc1, shown below, is the same as in our previous example. All network interfaces will be in Area 0:

```
cpc1#  vlan create 2 vlan2 untagged=4-5
cpc1#  vlan create 3 vlan3 untagged=6-8
cpc1#  vlan create 4 vlan4 untagged=9-12
cpc1#  vlan create 5 vlan5 untagged=13-16
cpc1#  vlan remove 1 untagged=4-16
cpc1#  ip config sw1 172.16.1.1 255.255.255.0 2
cpc1#  ip config sw2 172.16.2.1 255.255.255.0 3
cpc1#  ip config sw3 172.16.3.1 255.255.255.0 4
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
cpc1#  ip config sw4 172.16.4.1 255.255.255.0 5
cpc1#  route ospf id 172.16.1.1
cpc1#  route enable ospf
cpc1#  route ospf area add 0.0.0.0
cpc1#  route ospf interface add 172.16.1.1 0.0.0.0
cpc1#  route ospf interface add 172.16.2.1 0.0.0.0
cpc1#  route ospf interface add 172.16.3.1 0.0.0.0
cpc1#  route ospf interface add 172.16.4.1 0.0.0.0
cpc1#  save
```

We will configure the cpc2 as an Area Border Router, and place the sw5 interface in Area 1. The remaining network interfaces, sw1-sw4, will remain in Area 0. The configuration for cpc2 looks like the following:

```
cpc2#  vlan create 2 vlan2 untagged=5-7
cpc2#  vlan create 3 vlan3 untagged=8-10
cpc2#  vlan create 4 vlan4 untagged=11-14
cpc2#  vlan create 5 vlan5 untagged=15-20
cpc2#  vlan create 6 vlan6 untagged=21-22
cpc2#  vlan remove 1 untagged=5-22
cpc2#  ip config sw1 172.16.1.2 255.255.255.0 2
cpc2#  ip config sw2 172.16.22.2 255.255.255.0 3
cpc2#  ip config sw3 172.16.23.2 255.255.255.0 4
cpc2#  ip config sw4 172.16.24.2 255.255.255.0 5
cpc2#  ip config sw5 172.16.30.2 255.255.255.0 6
```

The following group of commands will enable OSPF on cpc2, configure areas 0 and 1, associate interfaces sw1-4 with area 0 and sw5 with area 1, and configure cpc2 as an Area Border Router:

```
cpc2#  route ospf id 172.16.1.2
cpc2#  route enable ospf
cpc2#  route ospf area add 0.0.0.0
cpc2#  route ospf area add 0.0.0.1
cpc2#  route ospf interface add 172.16.1.2 0.0.0.0
cpc2#  route ospf interface add 172.16.22.2 0.0.0.0
cpc2#  route ospf interface add 172.16.23.2 0.0.0.0
cpc2#  route ospf interface add 172.16.24.2 0.0.0.0
cpc2#  route ospf interface add 172.16.30.2 0.0.0.0
cpc2#  route ospf asborder on
cpc2#  save
```

We will configure cpc3 for area 1 rather than area 0. The configuration for cpc3 looks like the following:

```
cpc3#  vlan create 2 vlan2 untagged=1-7
cpc3#  vlan create 3 vlan3 untagged=8-16
cpc3#  vlan create 4 vlan4 untagged=17-20
cpc3#  vlan remove 1 untagged=1-20
cpc3#  ip config sw1 172.16.30.3 255.255.255.0 2
cpc3#  ip config sw2 172.16.41.3 255.255.255.0 3
cpc3#  ip config sw3 172.16.42.3 255.255.255.0 4
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The following commands will create area 1 on cpc 3 and configure sw1-sw3 for area 1.

```
cpc3#  route ospf id 172.16.30.3
cpc3#  route enable ospf
cpc3#  route ospf area add 0.0.0.1
cpc3#  route ospf interface area sw1 0.0.0.1
cpc3#  route ospf interface area sw2 0.0.0.1
cpc3#  route ospf interface area sw3 0.0.0.1
cpc3#  save
```

Because cpc2 has network interfaces in both area 0 and area 1, it is configured as an Area Border Router (ABR). On the other hand, cpc1 and cpc3 are internal to area 0 and area 1, respectively.

Again, we can use various “show” commands to verify that our settings are correct. First, we can verify that cpc2, an Area Border Router, established Neighbor relationships with both cpc1 and cpc3 by executing the “show neighbor” command:

```
cpc2#  route ospf show neighbor

IP Address   Router ID    Optns  Pri  State  Evnt  Dynamic
-------------------------------------------------------------
172.16.1.1   172.16.1.1   2      1    full   866   on
172.16.30.3  172.16.30.3  2      1    full   874   on
```

Notice that cpc2 established “full” relationships with both cpc1 and cpc3.

To verify that the sw5 network interface driver has been configured for area 1, use the “interface show” command

```
cpc2#  route ospf interface show

Iface  IP           Area     State               Admin State
-----------------------------------------------------------
sw1    172.16.1.2   0.0.0.0  designated router   on
sw2    172.16.22.2  0.0.0.0  designated router   on
sw3    172.16.23.2  0.0.0.0  designated router   on
sw4    172.16.24.2  0.0.0.0  designated router   on
sw5    172.16.30.2  0.0.0.1  designated router   on
```

Notice that the area ID for sw5 is 1, while sw1-sw4 are configured for area 0. We can now determine whether cpc1 and cpc3 have advertised their routes to cpc2 by using the “route dump” command:

```
cpc2#  route dump

Destination  Subnet Mask      Next Hop     Age   Met  Prot
-------------------------------------------------------------
127.0.0.1    255.255.255.255  127.0.0.1    9964  0    local
172.16.1.0   255.255.255.0    172.16.1.2   9951  0    local
172.16.1.1   255.255.255.255  172.16.1.2   9920  0    other
172.16.2.0   255.255.255.0    172.16.1.1   6129  1    ospf
172.16.3.0   255.255.255.0    172.16.1.1   6129  1    ospf
172.16.4.0   255.255.255.0    172.16.1.1   6129  1    ospf
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
172.16.22.0  255.255.255.0    172.16.22.2  9952  0    local
172.16.23.0  255.255.255.0    172.16.23.2  9952  0    local
172.16.24.0  255.255.255.0    172.16.24.2  9952  0    local
172.16.30.0  255.255.255.0    172.16.30.2  9952  0    local
172.16.30.3  255.255.255.255  172.16.30.2  9925  0    other
172.16.41.0  255.255.255.0    172.16.30.3  9913  1    ospf
172.16.42.0  255.255.255.0    172.16.30.3  9913  1    ospf
```

The cpc2 routing table shows three networks advertised by OSPF from cpc1 and two networks advertised by OSPF from cpc3.

Finally, we can examine the Link State Database on cpc2 by using the “route ospf show database” command.

```
cpc2#  route ospf show database

Router Link Status

Area     Link ID     Router ID   Age  Sequence      Chksum
-------------------------------------------------------------
0.0.0.0  172.16.1.1  172.16.1.1  512  0x080000266   0x9ce0
0.0.0.0  172.16.1.2  172.16.1.2  476  0x080000043   0xb3ac
0.0.0.1  172.16.1.2  172.16.1.2  484  0x080000041   0x4293
0.0.0.1  172.16.30.3 172.16.30.3 572  0x08000002a   0x744e

Net Link States

Area     Link ID     Router ID   Age  Sequence      Chksum
-------------------------------------------------------------
0.0.0.0  172.16.1.2  172.16.1.2  479  0x080000042   0x52c8
0.0.0.0  172.16.2.1  172.16.1.1  409  0x080000267   0xad0b
0.0.0.0  172.16.3.1  172.16.1.1  410  0x080000268   0xa016
0.0.0.0  172.16.4.1  172.16.1.1  410  0x080000269   0x9321
0.0.0.0  172.16.22.2 172.16.1.2  471  0x080000045   0x15b0
0.0.0.0  172.16.23.2 172.16.1.2  471  0x080000046   0x08bb
0.0.0.0  172.16.24.2 172.16.1.2  471  0x080000047   0xfac6
0.0.0.1  172.16.30.3 172.16.30.3 577  0x080000029   0x8652
0.0.0.1  172.16.41.3 172.16.30.3 590  0x080000027   0xb3df
0.0.0.1  172.16.42.3 172.16.30.3 590  0x080000028   0xa6ea

Summary Net Link States

Area     Link ID     Router ID   Age  Sequence      Chksum
-------------------------------------------------------------
0.0.0.0  0.0.0.0     172.16.1.2  495  0x080000040   0x510c
0.0.0.1  0.0.0.0     172.16.1.2  476  0x080000044   0x4910
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Configuring OSPF Timers

OSPF uses three timers to age out entries from its topology table:

- The Hello timer specifies the length of time, in seconds, between the Hello packets that the router sends on the interface. The default Hello timer is 10 seconds.
- The Dead timer specifies how long a router's neighbor will wait to receive a Hello packet before declaring the router down. The default Dead timer is 40 seconds (4 times the Hello timer).
- The Wait timer specifies how long the router waits before it flushes an entry out of its routing table. The Wait timer always equals the Dead timer. You may not change this timer directly, but if you change the Dead timer, you also indirectly change the Wait timer, since one always equals the other.

You may change the OSPF timers, although it is not recommended. You should remember that if you change the Hello or Dead timer on one router, you need to change the same timer on all routers connected to this interface, or else these routers will not form adjacencies.

The following commands will set the Hello timer to 15 seconds and the Dead timer to 60 seconds on cpc1 and cpc2:

```
cpc1#  route ospf interface hello 172.16.1.1 15
cpc1#  route ospf interface dead 172.16.1.1 60
cpc2#  route ospf interface hello 172.16.1.2 15
cpc2#  route ospf interface dead 172.16.1.2 60
```

Notice that the Hello and Dead timers on both routers are configured to be the same. This is a requirement for the two routers to form neighbor relationships.

Configuring Authentication

By default, OSPF does not use authentication. If you enable authentication, remember that the same authentication must be set on all interfaces which participate in the OSPF process. The following commands will set a simple password authentication on cpc1 and cpc2, using the key "connie":

```
cpc1#  route ospf interface authtype 172.16.1.1 simplePassword
cpc1#  route ospf interface authkey 172.16.1.1 connie
cpc2#  route ospf interface authtype 172.16.1.2 simplePassword
cpc2#  route ospf interface authkey 172.16.1.2 connie
cpc2#  save
```

Setting a Virtual Link

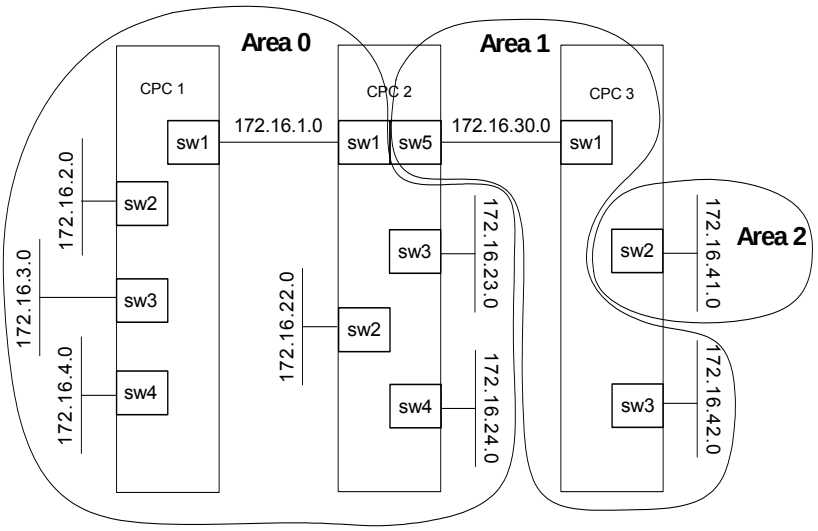
In a properly configured network, all areas must connect to Area 0. If we modify the multi-area configuration shown in Figure 13-9: "Multiple Area Configuration" on page 348 by creating a new area, Area 2, and then set cpc3's sw2 to be in Area 2, we must then create a virtual link that will connect Area 2 to Area 0.

First we need to create Area 2, and then set cpc3's sw2 interface to be in Area 2:

```
cpc3#  route ospf area add 0.0.0.2
cpc3#  route ospf interface add 172.16.41.3 0.0.0.2
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 13-10: Virtual Link Configuration



In order for Area 2 to communicate with the rest of the network, we need to create a virtual link that connects Area 2 with Area 0. When creating a virtual link, we must point to a Router ID, rather than to the IP address of the network interface that connects the router to a transit area. To verify the Router ID, execute the “route ospf show general” command. In our example, the Router ID for cpc2 is 172.16.1.2 and the Router ID for cpc3 is 172.16.30.3. The following two commands will set up a virtual link from Area 2 to Area 0, through Area 1:

```
cpc2#  route ospf virtual add 1 172.16.30.3
cpc3#  route ospf virtual add 1 172.16.1.2
```

Notice that cpc2’s virtual link points to cpc3 and vice versa.

You can examine the virtual link settings on cpc2 and cpc3 by executing the following command:

```
cpc2#  route ospf virtual show

Area     Neighbor     Delay  Retrans  Hello  Dead  Events  State
-----------------------------------------------------------------
0.0.0.1  172.16.30.3  1      5        10     60    1       up

cpc3#  route ospf virtual show
Area     Neighbor     Delay  Retrans  Hello  Dead  Events  State
-----------------------------------------------------------------
0.0.0.1  172.16.1.2   1      5        10     60    1       up
```

In both cases, the “Area” is Area 1, which is a transit through which we created the virtual link. The “Neighbor” is an IP address of the adjacent switch, with which a virtual link is being formed. Also notice that both the Hello and Dead intervals match on both switches.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

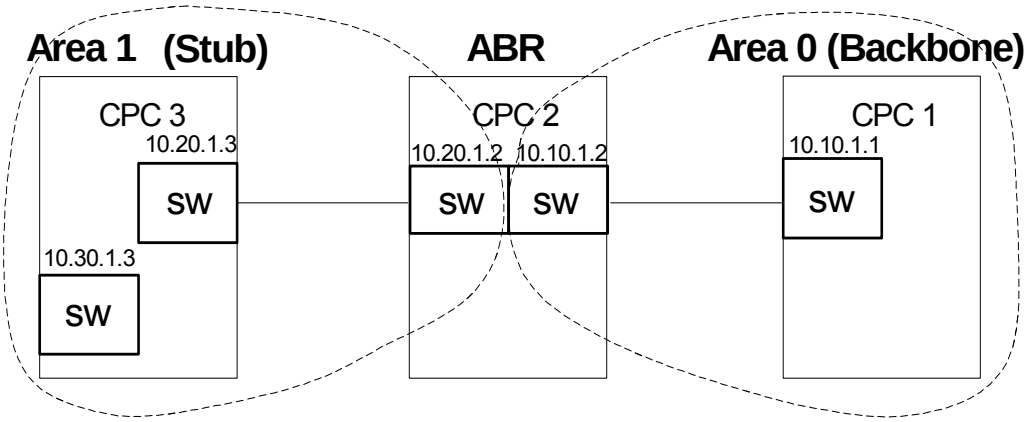
Setting a Stub Area

A stub area prevents ASBR external LSAs (Type 5) and ASBR summary LSAs (Type 4) from flooding the routers contained within the area. If many external links are present on a network, performance may improve noticeably by configuring a stub area, and thus reducing the size of the routing table and databases. However, stub areas have inter-area and intra-area routes. In order to reach outside networks, routers in the stub area use a default route (0.0.0.0) injected into the area by the Area Border Router (ABR). The default route is provided whether or not an alternate route has been configured. This default route will not appear in the ABR routing table, but it will appear in the OSPF database and routing table. It will also appear in the OSPF databases and routing tables of other routers within the stub area.

All routers in the stub area must have the same stub configuration or they will not be able to create adjacencies. When the “stub” command is executed, a special bit (an E bit) is set to zero in the Hello packet. All routers must agree on this setting or they will not become neighbors.

Following is a sample configuration:

Figure 13-11: Stub Area



In Figure 13-11: “Stub Area”, cpc1 belongs to backbone Area 0, and cpc3 belongs to Area 1, a stub area. Cpc2 is an Area Border Router (ABR) connecting Area 1 to Area 0.

In order to configure cpc2 as an ABR to a stub area, we need to create Area 0 and Area 1, with Area 1 configured as importNoExternal:

```
cpc2#  route ospf area 0 add
cpc2#  route ospf area 1 add importNoExternal
```

Note: *Once an area exists, you may not change its LSA options. In our example, if Area 1 had already been configured as importExternal, we would have had to remove Area 1 and then create it again, specifying importNoExternal.*

Next, we need to make Area 1 a stub area on cpc2:

```
cpc2#  route ospf stub add 1
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Finally, we need to add network interfaces to Area 0 and Area 1. (Remember that in order to add interfaces to OSPF, they must first be created with the “ip config” command.)

```
cpc2#  route ospf interface add 10.10.1.2 0
cpc2#  route ospf interface add 10.20.1.2 1
```

The configuration for cpc3 is as follows:

```
cpc3#   route ospf area 1 add importNoExternal
cpc3#   route ospf  stub 1
cpc3#   route ospf interface add 10.20.1.3 1
cpc3#   route ospf interface add 10.30.1.3 1
```

When Area 1 is properly configured as a stub area, cpc3 will have a default route (0.0.0.0) in its routing table pointing to cpc2, and cpc2 will have the same default route pointing to cpc3. This default route is injected into the stub area by the ABR, and occurs regardless of any routes configured by the user.

Limitations of Performance Technologies’ OSPF

The current Performance Technologies OSPF implementation has the following limitations:

The Performance Technologies OSPF does allow for modifying, maintaining and configuring OSPF at run-time. All changes to the OSPF algorithm take immediate effect without rebooting the switch. Of course, all configuration changes need to be saved so they can be properly restored when the switch reboots. The only exception is changing the OSPF Router ID, which requires OSPF to be restarted.

There are some RFC1850 MIB objects that are not supported in this implementation:

- ospfMulticastExtensions
- ospfDemandExtensions
- ospfAreaRangeAreaID
- ospfAreaRangeNet
- ospfAreaRangeMask
- ospfAreaRangeStatus
- ospfAreaRangeEffect

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

14

Virtual Router Redundancy Protocol

Overview

This section describes the Virtual Router Redundancy Protocol (VRRP). The key topics in this chapter include:

- “VRRP Overview” on page 357
- ‘“Terminology” on page 358
- “Configuring the Simple VRRP Interface Router” on page 360
- “Load Sharing VRRP Interface Example” on page 363

VRRP Overview

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the Master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without having to configure dynamic routing or router discovery protocols on every end-host.

There are a number of methods that an end-host can use to determine its first hop router towards a particular IP destination. These include running (or snooping) a dynamic routing protocol such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) version 2, running an ICMP router discovery client (DISC), or using a statically configured default route. Running a dynamic routing protocol on every end-host may not be feasible for a

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

number of reasons, including administrative overhead, processing overhead, security issues, or lack of a protocol implementation for some platforms. Neighbor or router discovery protocols may require active participation by all hosts on a network, leading to large timer values to reduce protocol overhead in the face of large numbers of hosts. This can result in a significant delay in the detection of a lost (i.e., dead) neighbor, which may introduce unacceptably long “black hole” periods

The use of a statically configured default route is quite popular; it minimizes configuration and processing overhead on the end-host and is supported by virtually every IP implementation. This mode of operation is likely to persist as dynamic host configuration protocols (DHCP) are deployed, which typically provide configuration for an end-host IP address and default gateway. However, this creates a single point of failure. Loss of the default router results in a catastrophic event, isolating all end-hosts that are unable to detect any alternate path that may be available. The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure inherent in the static default routed environment.

Terminology

VRRP Router: Each physical router running VRRP is known as a VRRP Router. Two or more VRRP Routers can be configured to form a Virtual Interface Router. Each VRRP Router may participate in one or more Virtual Interface Routers.

Virtual Interface Router: A Virtual Interface Router acts as a default or next-hop gateway for hosts on a LAN. Each Virtual Interface Router consists of a user-configured Virtual Router Identifier (VRID) and an IP address.

Virtual Router Identifier (VRID): The VRID is used to build the Virtual Router MAC Address. The five highest order octets of the Virtual Router MAC Address are the standard MAC prefix (00-00-5E-00-01) defined in RFC 2338. The VRID is used to form the lowest order octet.

IP Address Owner: One, but not more than one, of the VRRP Routers in a Virtual Interface Router may be configured as the IP Address Owner. This router has the Virtual Interface Router’s IP address as its real interface address. This router, when up, responds to packets addressed to the Virtual Interface Router’s IP address for ICMP pings, TCP connections, etc. The Performance Technologies implementation does not currently support IP Address Owner, although it will interoperate with another VRRP router that does.

Virtual Router Master: Within each Virtual Router, one of the VRRP routers is selected to be the Virtual Router Master. See “Determining Which VRRP Router is the Master” on page 360 for an explanation of the selection process. Note that if the IP Address Owner is available, then it will always become the Master.

The Virtual Router Master forwards packets sent to the Virtual Interface Router. It also responds to ARP requests with the Virtual Interface Router's IP address. Finally, it sends out periodic advertisements to let other VRRP Routers know it is alive and its priority (explained below).

Virtual Router Backup: Within a Virtual Router, the VRRP routers not selected to be the Master are known as Virtual Router Backups. Should the Virtual Router Master fail, one of the Virtual Router Backups becomes the Master and assumes its responsibilities.

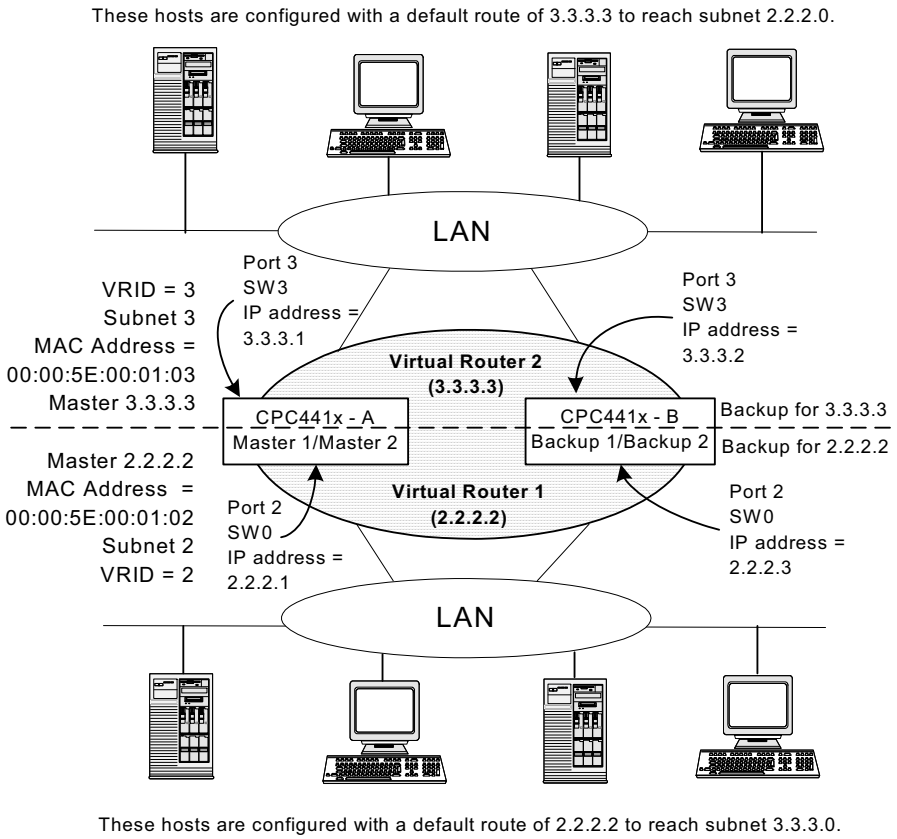
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Virtual Router Advertisement Interval: This is the period at which the VRRP Router sends VRRP Advertisement packets. If the Backup Router does not receive Advertisements after a number of intervals have elapsed, it will assume Mastership. The number of intervals to wait before assuming mastership is configurable by setting the 'Master Down Interval Counter'. See "Display or Set VRRP Master Down Interval Count" on page 260.

Note: *The Advertisement Interval must be configured the same on all routers configured to backup a specific VRID.*

The above points are illustrated in Figure 14-1: "Simple Virtual Interface Router Example". The switches in the diagram have been configured as VRRP Routers. They form a Virtual Interface Router.

Figure 14-1: Simple Virtual Interface Router Example



The servers and workstations shown in Figure 14-1 are configured with the Virtual Interface Router's IP address as their default gateway. The Master forwards packets destined to remote subnets and responds to ARP requests.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Determining Which VRRP Router is the Master

Each VRRP Router that is a Backup is configured with a priority between 1 - 254. According to the VRRP standard, an Owner has a priority = 255.

A bidding process determines which VRRP Router is the Master. The VRRP Router with the highest priority becomes the Master. Since Owners have a priority higher than the range permitted for Backups, the IP Address Owner, if any, is always the Master for the Virtual Interface Router as long as it is available.

The Master periodically sends out advertisements to an IP multicast address. As long as the Backups receive these advertisements, they remain in the backup state. If a Backup does not receive an advertisement for three advertisement intervals, it kicks off a bidding process to determine which VRRP router has the highest priority. The highest priority VRRP router takes over as Master.

If, at any time, a Backup determines that it has higher priority than the current Master does, it can preempt the Master, unless it is configured not to do so. In preemption, the Backup begins to send its own Advertisements. The current Master will see that the Backup has higher priority and stop functioning as the Master. The Backup will then see that the Master has stopped sending advertisements and assume the role of Master.

Note: *There are no acknowledgments sent from the Master to the Backup when it is determined that the Backup should become Master. The Backup will immediately transition to Master without waiting for the Master to first become Backup. This behavior by the protocol creates a possibility of a duplicate packet during the transition because both Routers for a brief interval could be Master.*

Configuring the Simple VRRP Interface Router

The Simple VRRP Interface Router example shows a redundant route between two subnets. Having a single CPC441x act as master router on both subnets with another CPC441x acting as backup for both subnets provides fault tolerance. If the master router goes offline for any reason, the backup is ready to become master for both subnets.

Before setting up VRRP there are several other protocols and settings that need to be configured first. Static VLANs, GVRP, Switch Interfaces, and Spanning Tree are all features of the CPC441x that play a major role in the operation of VRRP. In order for VRRP to operate correctly, these features must be configured prior to VRRP.

Configuring VLANs

The first configuration step is to set up static VLANs. There must be an autonomous VLAN for each subnet the switch routes to. This configuration will create non-overlapping VLANs and provide Broadcast/Multicast containment on each subnet. See Chapter 10, “VLANs,” on page 303.

For the purposes of this example we will assume that each CPC441x has a connection on port 2 to subnet 2.2.2.0 with a subnet mask of 255.255.255.0, that port 3 on each CPC441x has a connection to subnet 3.3.3.0 with a subnet mask of 255.255.255.0, and that the switch has default settings.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The commands to set up the VLANs for the simple VRRP Interface Router in Figure 14-1: “Simple Virtual Interface Router Example” on page 359 are:

```
vlan remove 1 untagged=2–3
vlan create 2 vlan2 untagged=2
vlan create 3 vlan3 untagged=3
```

By default, PVIDs are assigned to the ports corresponding to their respective VIDs: Port 2 has a PVID of 2 and Port 3 has a PVID of 3.

Configuring GVRP (GARP VLAN Registration Protocol)

The next feature to configure is GVRP. In order to achieve Broadcast/Multicast containment at Layer 3 on the VLANs, GVRP must be disabled. Disabling GVRP prevents any GVRP-aware devices from joining the VLANs configured on the switch. If joining were allowed, then VLAN port membership could be altered and the subnet boundaries could be crossed.

```
gvrp set all off
```

As stated above, the VLAN Create commands have by default configured the two associated ports with PVIDs that correspond to the VIDs. The following commands could be used to explicitly assign the same PVIDs independently of the VLAN Create command:

```
gvrp pvid 2 2
gvrp pvid 3 3
```

See “VLAN Identification” on page 304 for information on PVIDs, and “Associate a PVID with a Set of Ports” on page 127.

Configuring Switch Interfaces

The CPC441x’s switch interfaces must be configured in order for the switch to route between subnets. Each interface must also be associated with the corresponding VLAN. In this example, VLAN2 has a connection on port 2 to subnet 2.2.2.0 (any interface that doesn’t have an IP address can be used). CPC441xA uses sw0 and sets its IP address to be 2.2.2.1. Port 3 is in VLAN3, and is attached to the 3.3.3.0 subnet. Both CPC441x switches must have an interface configured to these VLANs. If the interface is not attached to the proper VLAN, routing between subnet 2.2.2.0 and 3.3.3.0 will not occur.

For CPC441xA:

```
ip config sw0 2.2.2.1 255.255.255.0 vid=2
ip config sw3 3.3.3.1 255.255.255.0 vid=3
```

For CPC441xB:

```
ip config sw0 2.2.2.3 255.255.255.0 vid=2
ip config sw3 3.3.3.2 255.255.255.0 vid=3
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Configuring VRRP

In this example, CPC441xA is acting as the master for both subnets. If it fails for any reason, CPC441xB will take over the responsibility of forwarding packets destined to the Virtual Router's IP address, and answering any ARP requests for the Virtual Router's IP address. The Virtual Router's IP address must correspond with the correct switch interface. In this example, sw0 is attached to the 2.2.2.0 subnet and thus we have the router's IP address 2.2.2.2 matched with sw0. The same is true for sw3 and 3.3.3.3. The CPC441xA is configured with a priority of 254, while the CPC441xB has a priority of 25. This difference in priority is what ensures that the CPC441xA becomes the master.

For CPC441xA:

```
vrrp set 2 sw0 2.2.2.2 priority=254
vrrp set 3 sw3 3.3.3.3 priority=254
vrrp enable 2 sw0 on
vrrp enable 3 sw3 on
```

For CPC441xB:

```
vrrp set 2 sw0 2.2.2.2 priority=25
vrrp set 3 sw3 3.3.3.3 priority=25
vrrp enable 2 sw0 on
vrrp enable 3 sw3 on
```

Spanning Tree

Spanning Tree is used to remove loops on networks. The CPC441x currently runs a single Spanning Tree which does not take into account VLAN boundaries. In our example there is a loop which Spanning Tree, enabled by default, will block. In order for VRRP to function properly, Spanning Tree must be disabled on the ports that have created the loop.

However, disabling Spanning Tree prior to setting up VLANs, GVRP, and switch interfaces may cause network problems due to the loop in the configuration.

The "span port vlan" command will disable Spanning Tree on the specified ports just like the span port enable. The difference is that when a reset occurs on the switch, Spanning Tree is enabled on the ports until VLANs and interfaces are configured from settings in NVRAM. Then the Spanning Tree algorithm on the specific ports is disabled.

For both CPC441xs:

```
span port vlan 2,3 off
```

The final step is to set up the hosts so they use the proper default route for each subnet. Hosts on the 2.2.2.0 subnet must have a default route to 2.2.2.2. The hosts on the 3.3.3.0 subnet need a default route to 3.3.3.3.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Load Sharing VRRP Interface Example

Figure 14-2: “Balanced Virtual Interface Router Example” on page 365 gives an example of using the two CPC441x’s in a load sharing environment. Each CPC441x acts as both Master and Backup for the two Virtual Router Interfaces. It appears as two distinct routers to the LAN. This allows each server/workstation to use a separate gateway address so as not to overload one CPC441x while allowing the other to be idle.

As in the previous example, Spanning Tree, VLANs, GVRP, and switch interfaces need to be configured prior to VRRP (see “Configuring the Simple VRRP Interface Router” on page 360).

VLANs

For both CPC441xs:

```
vlan remove 1 untagged=13-26
vlan create 2 vlan2 untagged=13-26
```

GVRP

For both CPC441xs:

```
gvrp set all off
```

Switch Interfaces

For CPC441xA:

```
ip config sw0 192.168.1.101 255.255.255.0 vid=1
ip config sw1 192.168.17.101 255.255.255.0 vid=2
```

For CPC441xB:

```
ip config sw0 192.168.1.102 255.255.255.0 vid=1
ip config sw1 192.168.17.102 255.255.255.0 vid=2
```

Spanning Tree

Spanning Tree must be disabled on those ports that will connect to the LANs. For example, if CPC441xA has a connection on port 1 to subnet 192.168.1.0 and a connection on port 5 to subnet 192.168.17.0, then these ports must have Spanning Tree disabled. The following command will achieve this:

```
span port vlan 1,5 off
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

How to Configure the Load Sharing VRRP Interface Router

The following commands will set up CPC441xA (left in Figure 14-2: “Balanced Virtual Interface Router Example” on page 365):

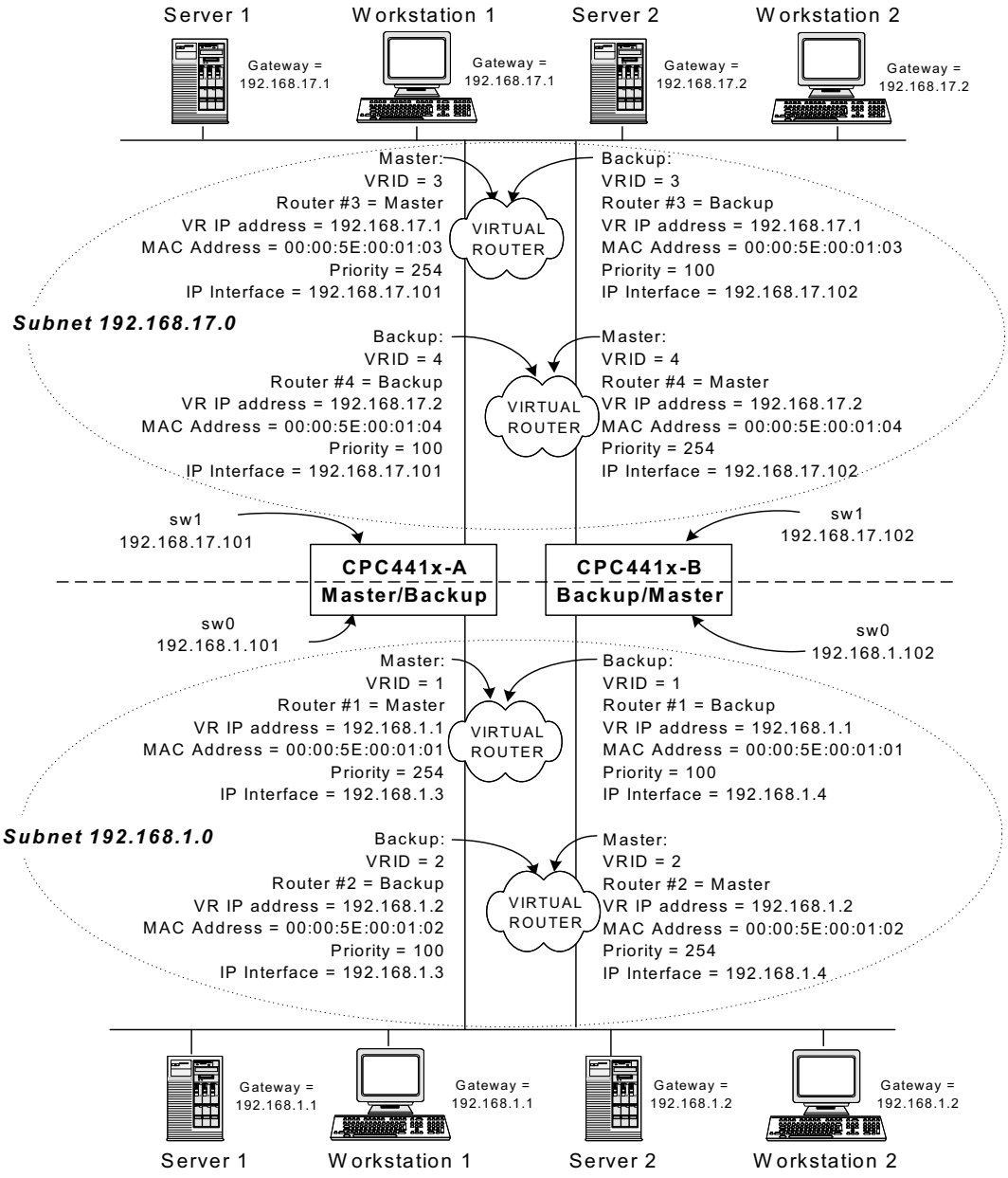
```
vrrp set 1 sw0 192.168.1.1 priority=254
vrrp set 2 sw0 192.168.1.2
vrrp set 3 sw1 192.168.17.1 priority=254
vrrp set 4 sw1 192.168.17.2
vrrp enable 1 sw0 on
vrrp enable 2 sw0 on
vrrp enable 3 sw1 on
vrrp enable 4 sw1 on
```

The following commands will set up CPC441xB (right in Figure 14-2):

```
vrrp set 2 sw0 192.168.1.2 priority=254
vrrp set 1 sw0 192.168.1.1
vrrp set 4 sw1 192.168.17.2 priority=254
vrrp set 3 sw1 192.168.17.1
vrrp enable 1 sw0 on
vrrp enable 2 sw0 on
vrrp enable 3 sw1 on
vrrp enable 4 sw1 on
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 14-2: Balanced Virtual Interface Router Example



Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

15

Spanning Tree

Overview

This chapter contains information on configuring and using Spanning Tree on the CPC441x.

The key topics in this chapter include:

- "Spanning Tree (STP)" on page 368
- "Fast Port" on page 369
- "Fast Uplink" on page 369
- "Port Path Cost" on page 372
- "Rapid Spanning Tree" on page 373
- "Differences Between RSTP and STP" on page 379
- "RSTP Configuration Example" on page 381

Note: *An excellent reference on the implementation and design of networks using Spanning Tree functions is "The Switch Book: The Complete Guide to LAN Switching Technology" by Rich Seifert (May 2000), John Wiley & Sons; ISBN: 0471345865.*

General

Spanning Tree is a link management protocol that provides path redundancy while preventing loops in a network. It is defined by two distinct IEEE algorithms:

- 802.1D-1998 Spanning Tree Algorithm (STP) – Spanning Tree version 0
- 802.1D-2004 Rapid Spanning Tree Algorithm (RSTP) – Spanning Tree version 2

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Both algorithms perform the same functions, but they differ “under the hood.” RSTP can interoperate with both STP and RSTP devices, but when RSTP operates in STP-compatible mode, it behaves like STP but does not run STP code. When RSTP detects a legacy STP device on a port, it configures the port to operate in STP-compatible mode; specifically, it uses STP-style Bridge Protocol Data Units (BPDUs), and disables certain RSTP features, such as sync handshake. For more information on the operation of RSTP, see “Rapid Spanning Tree” on page 373, and the IEEE 802.1D-2004 specification.

The CPC441x can run either of the two algorithms, but only one at a time. By default, the CPC441x powers up running STP; to switch between the two algorithms, the user must save the new settings and reboot the switch.

Spanning Tree (STP)

For an Ethernet network to function properly, only one active path must exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP can logically break such loops and prevent looping traffic from clogging the network. The dynamic control of the topology provides continued network operation in the presence of redundant or unintended looping paths.

The CPC441x includes a Spanning Tree Algorithm (STA) that uses the IEEE 802.1D Spanning Tree Protocol (STP). The CPC441x uses the Spanning Tree Algorithm (STA) to automatically detect network loops and block redundant connections. In addition, the STA detects hardware and cable failures, and re-activates blocked redundant connections when needed. A single STP algorithm runs on each switch module.

By default, Spanning Tree is enabled on the CPC441x. To disable Spanning Tree, execute the following command:

```
# span bridge enable off
```

The following command will re-enable Spanning Tree:

```
# span bridge enable on
```

When you disable Spanning Tree, all Bridge Protocol Data Units (BPDUs) received by the switch will be sent to the CPU and replicated to all ports that have the Spanning Tree Protocol enabled on them, i.e., the BPDUs will be forwarded to other ports. This allows other switches that are running Spanning Tree to detect a loop. If you do not want BPDUs to be replicated on a port, then disable the protocol on that port(s) with the “span port protocol enable” command.

To avoid incurring the delay sometimes associated with Spanning Tree convergence (30 - 50 seconds), use Fast Port or Fast Uplink (see below), or disable Spanning Tree only on those ports that are not connected to other switches or bridges.

To disable the Spanning Tree protocol on ports 1-5, use the following command:

```
# span port protocol enable 1-5 off
```

To place ports 1-5 in the DISABLED Spanning Tree state, use the following command:

```
# span port enable 1-5 off
```

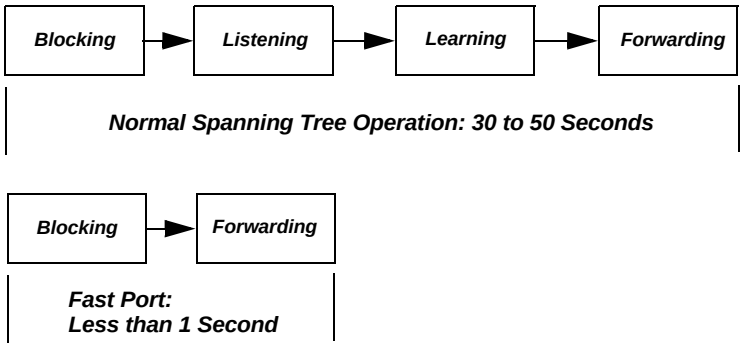

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Fast Port

When Spanning Tree detects a network topology change, a network traffic delay can occur that lasts from 30 to 50 seconds, during which the Spanning Tree Algorithm moves through the four states shown in Figure 15-1: “Effect of Fast Port on Spanning Tree Convergence”. A 30-50 second delay can appear to be a network failure, and can cause application timeouts during client/server operations.

The Fast Port function provides faster Spanning Tree recovery, possibly preventing application timeout during Spanning Tree operation. Fast Port skips over the Listen and Learn states, allowing transitions directly from a Blocking state to a Forwarding state. See Figure 15-1: “Effect of Fast Port on Spanning Tree Convergence”.

Figure 15-1: Effect of Fast Port on Spanning Tree Convergence



Fast Port should be enabled only on ports connected to end-stations. Do not enable Fast Port on ports that are connected to network devices with multiple network connections where the propagation of loops is possible.

The CPC441x allows enabling the Fast Port feature on each port independently. For example, to enable Fast Port on ports 1 - 5, use the following command:

```
# span port fast 1-5 on
```

Fast Uplink

Fast Uplink is an enhancement to the Spanning Tree Protocol that provides fast convergence whenever STP picks a new Root Port. STP will select a new Root Port automatically when a link or switch fails or when STP parameters change. By default, Fast Uplink is disabled. The main benefit of the Fast Uplink is to protect against a link failure on the Root Port. In this case, Fast Uplink chooses one of the blocked ports (providing a redundant connection to the Root Bridge) to become a new Root Port.

The Spanning Tree Algorithm (STA) blocks all redundant connections (to the Root Bridge) to disallow loops. When the active link fails, the STA will activate the redundant connection which (without Fast Uplink) must go through blocking/listening/learning/forwarding states before it can forward user traffic. This transition from a blocking to a forwarding state might take between 30 and 50 seconds. The purpose of Fast Uplink is to bypass the regular STA transition and place the redundant link in a forwarding state when the active link failure is detected.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 15-2: “Fast Uplink Before Direct Link Failure” shows Bridge 2 having two redundant paths to the Root Bridge. It employs Fast Uplink in order to provide a fast convergence in case of a link failure. The Fast Uplink logic places ports 2 and 3 in a Fast Uplink group. Both ports provide a path to the Root Bridge (Bridge 1) with port 2 being a Root Port and port 3 a backup port. Spanning Tree places port 3 in a blocking state to eliminate loops. If the connection between bridge 2 and the Root Bridge breaks (the link on port 2 goes down), the Fast Uplink algorithm makes port 3 a new Root Port and places it in a Forwarding state bypassing standard Spanning Tree Listening and Learning states.

To enable Fast Uplink, use the following command:

```
# span bridge fast on
```

Figure 15-2: Fast Uplink Before Direct Link Failure

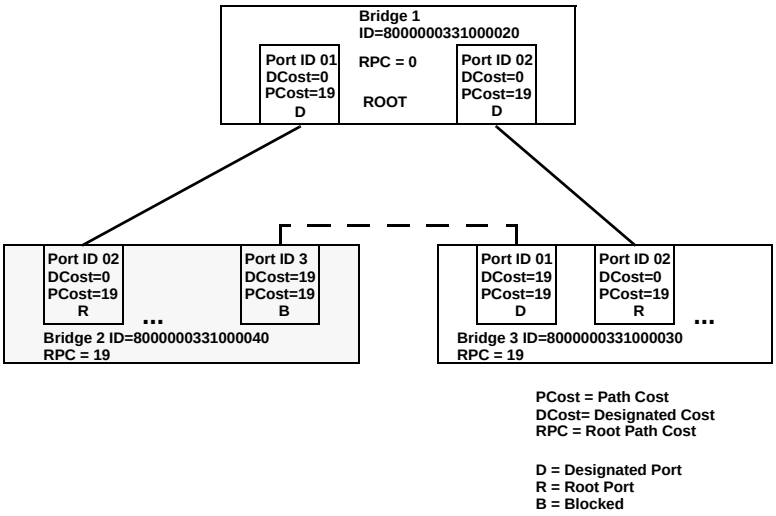
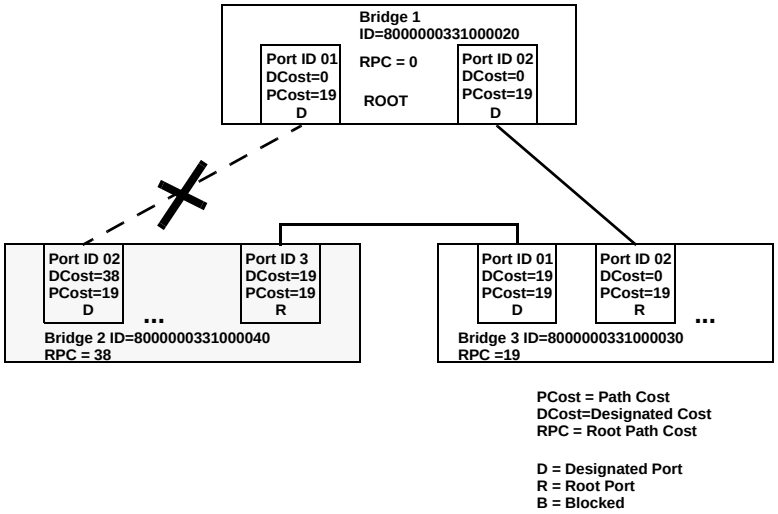


Figure 15-3: “Fast Uplink After Direct Link Failure” on page 371 shows the same network after a link failure of the currently active link which connects Bridge 2 with a Root Bridge.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 15-3: Fast Uplink After Direct Link Failure



When the connection between Bridge 2 and the Root Bridge (bridge 1) is restored, Fast Uplink reverts to the original configuration rapidly. Again, port 2 (on bridge 2) becomes a Root Port and port 3 (on bridge 3) is placed in a Blocking state. Although Fast Uplink restores the original Root Port (on bridge 2), and places it in a Forwarding state right away, port 1 on the Root Bridge (bridge 1) must transition through a Listening and Learning state before it is placed in a Forwarding state. This causes a network outage for about 30 seconds. It is important to understand that the Fast Uplink is designed to speed up a selection of a Root port and not Designated ports. In this example, when the connection between the Root Bridge (bridge 1) and bridge 2 is restored, the STA running on the Root Bridge detects that the link on port 1 is restored and makes port 1 a Designated port. Since Fast Uplink does not participate in a Designated port selection, this port needs to follow regular Spanning Tree state transitions (Blocking, Listening, Learning, Forwarding). In other words, Fast Uplink protects the bridged network from a link failure, but does not change the operation of the Spanning Tree during the recovery process. The repair of a broken link can, however, be scheduled such that the impact of 30–50 seconds down time is not critical. Network failure, on the other hand, cannot be scheduled. It is therefore important that the network downtime is minimized in the event of a network failure.

Fast Uplink Definitions

Fast Uplink uses the following definitions:

Fast Uplink Group

This is a group of ports consisting of a Root Port and all ports blocked by the STA. Fast Uplink group is created by the Fast Uplink algorithm and cannot be modified by the user. The user, however, can indirectly create a Fast Uplink group by providing redundant links between the bridge running the Fast Uplink algorithm and the Root Bridge.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Backup Root Port

This is a port that provides an alternate path to the Root Bridge. All bridge ports blocked by the STA fit this description and, therefore, are Backup Root Ports. If the link on the Root Port fails, one of the backup Root Ports will become the new Root Port. The Fast Uplink algorithm uses the same criteria as does the STA for choosing the next Root Port. In particular, the new Root Port will be the one having the shortest path to the Root Bridge.

If multiple backup ports have the same path cost to the root bridge, then the new Root Port will be the one with the better Designated Bridge ID. If multiple backup ports have the same path cost and the same Designated Bridge ID, then the Root Port will be the port with the better Designated Port ID. Finally, if multiple backup ports have the same path costs, Designated Bridge IDs, and Designated Port IDs, then the Root Port will be the port with the better local Port ID. The Port Identifiers for different ports on the same switch are guaranteed to be different and thus can serve as a tie-breaker. This new Root Port is further referred to as a `new_root_port`. The Root Port on which link has failed is further referred to as a Failed Root Port.

Port Path Cost

Port Path Cost contributes to the Root Path Cost (with Port Designated Cost) when the port is the root port. This value needs to be inversely proportional to the speed of the interface. The user may select one of the two pathcost styles: type 1 (defined in IEEE 802.1D-1998) or type 2 (defined in IEEE 802.1t, 802.1w and 802.1D-2003). Based on the pathcost style selected, Spanning Tree (STP or RSTP) will calculate the path cost based on the link speed. The two styles are compared in Table 15-1: “Port Path Costs”.

Table 15-1: Port Path Costs

Link Speed	Path Cost	
	Style 1	Style 2
10 Mbs	100	2 000 000
100 Mbs	19	200 000
1 Gbs	4	20 000
10 Gbs	2	2 000

The path cost style can be selected with the “span pathcost [style]” command, where “style” can be either 1 or 2. The change to the path cost style will not take effect until the configuration is saved and the switch is rebooted. The default path cost style is type 1 (the IEEE 802.1D-1998 path cost style). This means that whenever the CPC441x is restored to its factory default configuration with the “switch defaults” command, the path cost style will be restored to type 1 style. The following commands will change the path cost style from type 1 to type 2:

```
# span pathcost 2
# save
# switch reset
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Unlike the path cost style, the Port Path Cost is not durable (i.e., it is replaced by the factory default upon reboot), and cannot be written to via SNMP or CLI. The Port Path Cost is configured “under the hood” by Spanning Tree after detecting the speed and link. Except for selecting the path cost style, the user has no control over the path cost calculation.

Rapid Spanning Tree

Rapid Spanning Tree Algorithm and Protocol is an IEEE Spanning Tree standard that replaces the older Spanning Tree (802.1D-1998). Rapid Spanning Tree was originally defined in 802.1w, and later replaced the original STP in the 2003 release of 802.1D.

RSTP is not so much a new protocol as it is an improved and faster version of STP. It preserves all the basic concepts of STP, and interoperates with it as well. This section compares STP and RSTP, and describes how to configure RSTP on the CPC441x. In most cases, the user will not need to change Spanning Tree (STP/RSTP) settings. However, should adjustments be necessary, pay particular attention to the timer settings, in order to avoid difficulties.

Most Spanning Tree commands take effect immediately after they are entered. However, they will not be preserved after a reboot unless the user saves the configuration by executing the “save” command. Only two Spanning Tree commands do not take effect until the switch is reset: “span version,” which selects either of the Spanning Tree algorithms, and “span pathcost,” which selects the path cost style (see “Port Path Cost” on page 372).

To activate RSTP on the CPC441x, set the Spanning Tree version to 2, and then save and reboot the switch, using the following commands:

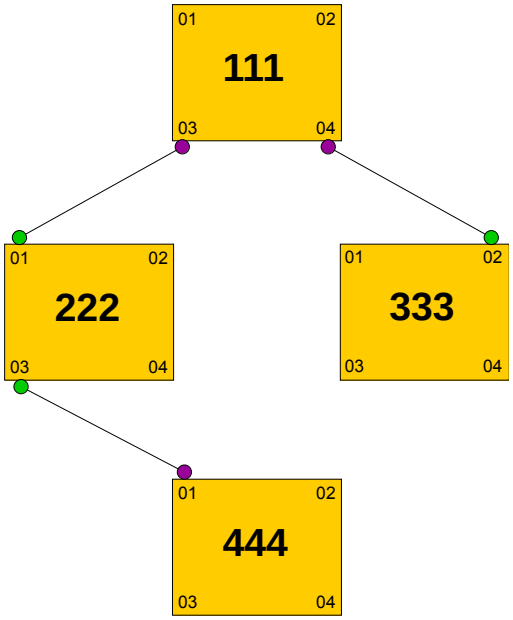
```
# span version 2
# save
# switch reset
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Tree Topology

Spanning Tree topology can be thought of as a tree: it includes a root (a Root Bridge), branches (LANs and Designated Switches), and leaves (End Nodes). On a tree there are no parts disconnected from any other part; that is, the tree encompasses all of its leaves, limbs, etc. In addition, there are no loops in a tree. If you trace a path from one leaf to any other leaf, you will find there is one, and only one, possible path. This is true of the Spanning Tree topology as well. It organizes and connects switches into a loop-free topology while leaving no segments isolated. Figure 15-4: “Loop-Free Topology” on page 374 depicts a loop-free network with active connections that span from the root (Root Bridge). In this example, switch 111 has been selected as a Root Bridge.

Figure 15-4: Loop-Free Topology



Root Bridge

Just as a tree has a root from which all branches spring, Spanning Tree has a Root Bridge. Only one Root Bridge can exist in any given network. Although any switch can be a Root Bridge, the switch with the best Bridge ID becomes the Root Bridge. There are two parts to the Bridge ID: a user-selected priority and the MAC address. The switch with the lowest numerical value of the priority component becomes the Root Bridge. If all switches have the same priority value, then the one with the lowest MAC address becomes the Root Bridge. The default value for the Bridge Priority is 32768, and the range is 0 to 65536. RSTP allows the priority to be set in increments of 4096, between 0 and 61440 (0, 4096, 8192, etc.). This is different from STP, where Bridge Priority can be set to any value between 0 and 65535. The following command will set the Bridge Priority to 4096, thereby making the switch a Root Bridge:

```
# span bridge priority 4096
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Timers

IEEE 802.1D specifies the relationship that must be maintained between the Spanning Tree timers. If one timer is modified, then the remaining timers must be adjusted to maintain this relationship. The following equations express this relationship:

```
2 x (Bridge_Forward_Delay – 1 second) >= Bridge_Max_Age
Bridge_Max_Age >= 2 x (Bridge_Hello_Time + 1 second)
```

The settings for Forward Delay and Max Age are adopted by all bridges and switches on the network from the Root Bridge. Therefore, to adjust these timers throughout the entire LAN, simply modify them on the Root Bridge.

Hello Time

The Root Bridge is responsible for transmitting BPDUs (Bridge Protocol Data Units, or small Hello packets), which aid other bridges and switches in maintaining a loop-free topology. BPDUs are transmitted every Hello time interval, which defaults to 2 seconds, and has an allowable range of 1 – 10 seconds (specified in hundredths of a second). The following command will change the Hello interval to 1 second:

```
# span bridge hello 100
```

Forward Delay Time

The Forward Delay timer specifies a transition interval from Discarding to Forwarding (specified in hundredths of a second). By default, Forward Delay is set to 15 seconds (“1500”), which means that in the worst case, ports may take up to 30 seconds (2 x 15) before transitioning to Forwarding. The allowable range is 4 – 30 seconds. The following command will change the Forward Delay to 10 seconds:

```
# span bridge delay 1000
```

Max Age Time

The Max Age timer ages out BPDUs that are too old. The 802.1D-1998 STP also uses this timer to determine how long the Root Port will wait for BPDUs on the Root Port before deciding that its connection to the Root Bridge is no longer there. The default value of the Max Age timer is 20 seconds, and its range is 6 – 40 seconds (specified in hundredths of a second). The following command will change the Max Age time to 15 seconds:

```
# span bridge maxage 1500
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Designated Bridges

A simple way to prevent loops in a network is to ensure that only one bridge is responsible for forwarding traffic from the direction of the root to any given link (branch). As long as only one active path from a root to any end node (leaf) exists, there will be no loops in the topology. The bridge responsible for forwarding traffic from the root to a given link is known as the Designated Bridge of that link.

Port States

There are three operational states assigned to each port by RSTP: Discarding, Learning and Forwarding. Discarding ports do not participate in the active topology and do not learn MAC addresses. Ports in Learning states learn MAC addresses, but do not forward user traffic. Ports in Forwarding states fully participate in both data forwarding and MAC learning. RSTP states differ somewhat from STP states. Table 15-2: “STP and RSTP Port States” depicts these differences.

Table 15-2: STP and RSTP Port States

STP Port State	RSTP Port State	Is Port Included in Active Topology?	Is Port Learning MAC Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

Port Roles

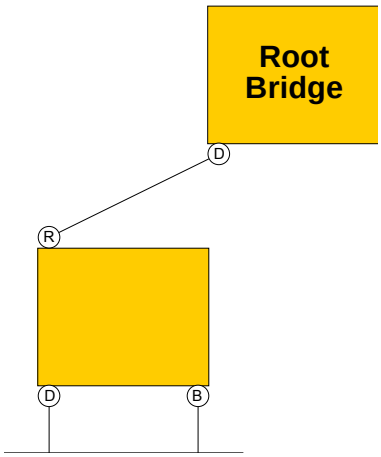
A port role is a function that STP and RSTP assigns to each port. The roles STP assigns are Root Port, Designated Port, and Blocking Port. RSTP splits the Blocking Port role into Backup and Alternate Port roles.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Root Port Role

A root port is the port closest to the root bridge in terms of path cost. When a switch has multiple paths connecting it to the root, the best path is determined based on the message priority vector carried inside the Bridged Protocol Data Unit (BPDU) and the receiving port ID. The port with the best priority vector becomes a root port while the remaining ports become alternates. Figure 15-5: “Port Roles” on page 377 depicts a root port (R).

Figure 15-5: Port Roles



Designated Port Role

A port is Designated if it can send the best BPDU on the segment to which it is connected. All bridges connected to a given segment listen to each other’s BPDUs and agree that the bridge sending the best BPDU is the designated bridge for the segment. Figure 15-5: “Port Roles” depicts a designated port (D).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

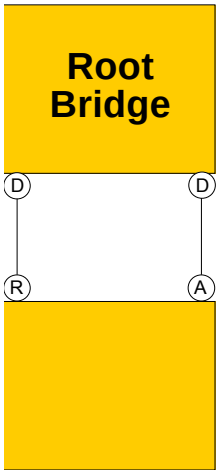
Alternate and Backup Port Roles

Alternate or backup ports do not forward user data, but serve as backups for the root and designated ports.

A backup port is connected to the same LAN as a designated port. Spanning Tree blocks backup ports since the designated port provides a better path from this LAN to the root bridge. Figure 15-5: “Port Roles” on page 377 shows a backup port (B).

An alternate port provides a redundant connection to the Root Bridge and can become a new Root Port in the event the current Root Port loses its connection to the Root Bridge. Figure 15-6: “Alternate Port” on page 378 shows the alternate port (A). In many cases, the alternate port can become a new root port and transition into the Forwarding state without a delay.

Figure 15-6: Alternate Port



BPDU Format

Bridges learn and exchange information about each other by sending small Hello packets called Bridge Protocol Data Units (BPDUs). There are some differences between STP and RSTP BPDUs.

STP BPDUs

STP uses two different BPDUs: Configuration BPDUs and Topology Change BPDUs. Configuration BPDUs originate from the root bridge every Hello time, and carry all information required to calculate the Spanning Tree topology. Other bridges listen for Configuration BPDUs on their root ports and forward them on their designated ports.

Topology Change BPDUs (TCN BPDUs) are sent in the direction of the root by the bridge which detected a topology change. When the root bridge receives a TCN BPDU, it must then inform other switches that a change has occurred in the current topology. It does so by setting a Topology Change (TC) flag in every BPDU it sends for a period of time (specified as Forward Delay + Max Age). When a switch receives a BPDU with a TC flag set, it switches its aging time from long to short in order to age out Filtering Database entries more rapidly.

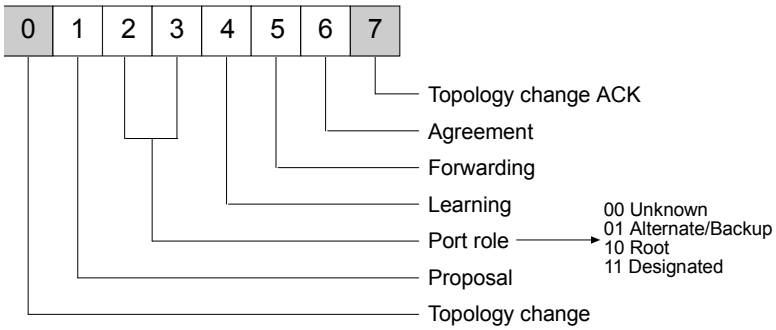
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

RSTP BPDUs

RSTP uses only one type of BPDU called RSTP BPDUs. They are similar to STP Configuration BPDUs with the exception of a type field set to “version 2” for RSTP or “version 0” for STP, and a flag field carrying additional information.

The STP BPDUs use only two flags: Topology Change (TC) and TC Acknowledgment (TCA). RSTP uses six additional bits to encode the role and the state of the port originating the BPDU, and two flags to handle the proposal/agreement mechanism. Figure 15-7: “Flag Fields for STP and RSTP” on page 379 shows the difference between STP and RSTP flag fields.

Figure 15-7: Flag Fields for STP and RSTP



Differences Between RSTP and STP

In many respects, STP and RSTP work the same. They reduce the bridged network to a single Spanning Tree topology in order to eliminate loops. Either algorithm reactivates redundant connections in the event of a link or component failure. The main difference is convergence time. While it may take STP 30 to 50 seconds to re-converge, RSTP does it in dramatically less time. In a carefully designed network, RSTP re-converges in less than a second. Although computation of the Spanning Tree is identical between STP and RSTP, there are differences in the behavior of the two algorithms.

Faster Filtering Database Aging

Switches listen for network traffic to learn which nodes (MAC addresses) are on which ports, then store these MAC-to-port entries in their databases. Later, when a frame arrives destined for one of these MAC address, it will be switched to the proper port. A database of these MAC-to-port entries is called a filtering database.

This database needs to be relearned every time a network topology change occurs or frames may be sent to the wrong ports. A topology change such as a link failure can cause some nodes to become connected to different switches. Even though no stations have been physically moved, it can appear to the switches as though stations have been lifted from one part of the network and reconnected into another. In order for traffic to reach these stations, switches need to age old information and relearn new node locations.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Switches running STP do not flush their filtering databases when they detect a topology change. Instead, they send Topology Change Notification BPDUs (TCN BPDUs) in the direction of the root bridge, which then informs all bridges a topology change has occurred. It may take several seconds before the TCN BPDU reaches the root bridge and several more seconds before the BPDUs (with the TC flag set) reach other bridges on the network. Even then, STP switches do not flush old information immediately. Instead, they switch their aging timer from long to short (a default value for the short timer is Forward Delay which equals 15 seconds). After this time, if entries are not refreshed they are removed from the database.

RSTP uses a more efficient mechanism to purge old information. First, every switch that detects a topology change sends BPDUs with the TC flag set. Secondly, the switch that detects a change purges old entries immediately. Finally, every switch that receives a BPDU with a TC flag set purges the old entries and relays this BPDU to other switches.

The improved speed with which switches eliminate old information is significant. Rather than waiting several seconds for the TCN BPDU to reach the root bridge, and several more seconds before the BPDU is received from the root bridge, and additional time for the Forward Delay time before aging out incorrect entries, switches purge old entries immediately and ask other switches to do the same.

BPDUs as “Keep-Alive”

STP switches do not generate their own BPDUs; they wait to receive them on their root ports and then relay them (after some processing) to their designated ports. If the STP Bridge does not receive a BPDU for a “max age time” (default 20 seconds), it declares the root bridge dead. It then assumes itself to be a root bridge and starts a new root bridge selection process.

An RSTP switch, on the other hand, sends its own BPDUs whether it received one on its root port or not. Instead of waiting for a “max age time,” an RSTP switch expects to receive a BPDU within three hello times. If the BPDU is not received within this time, the switch assumes it has lost connection with its neighbor. Of course, if a switch detects a loss of a link on a port, it immediately assumes its neighboring connection is lost.

Edge Ports

Spanning Tree takes great care to ensure that no loops exist in the network. That’s why switch ports will not send traffic until all switches agree on the network topology. There are, however, situations where ports connect directly to end stations – and cannot create loops. RSTP recognizes this, and allows configuring ports that do not connect to other bridges as edge ports. Edge ports do not need to transition through regular Spanning Tree states; they go directly to forwarding. If a switch detects a BPDU on an edge port, it automatically makes it a non-edge port. The following command illustrates how to set ports 5-10 to operate as edge ports:

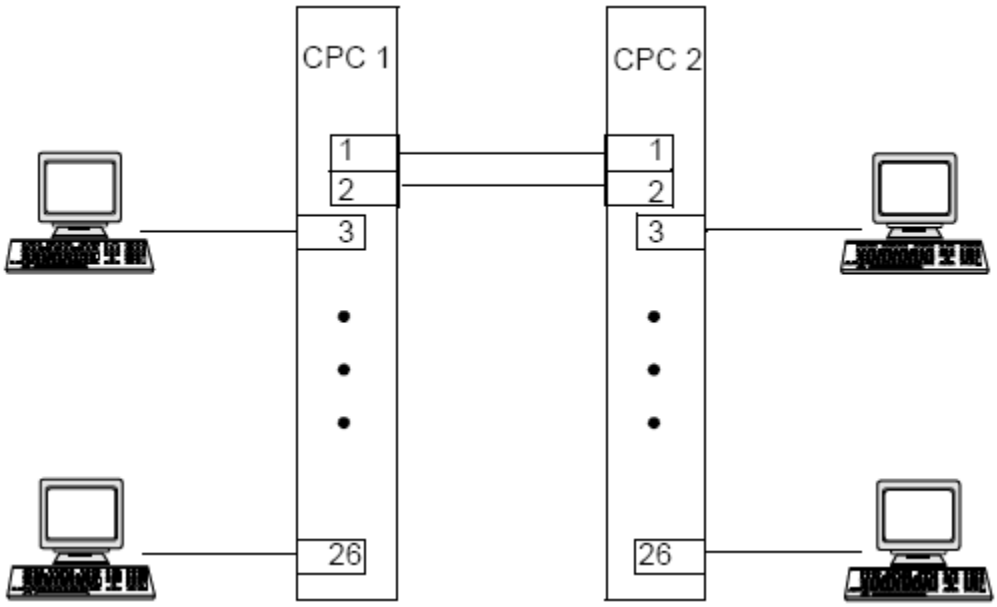
```
# span port edgeport 5-10 on
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

RSTP Configuration Example

To illustrate how to configure Rapid Spanning Tree, we'll use a simple bridged network comprising two CPC441xs: cpc1 and cpc2, connected together with two links such that port 1 on cpc1 connects to port 1 on cpc2 and port 2 on cpc1 connects to port 2 on cpc2. The remaining ports on both switches connect to hosts and end stations. We will configure cpc1 to be a Root Bridge. Then, we will change the Spanning Tree timers to adjust for the small diameter of our bridged network. Finally, we will configure ports 3-24 on both switches to be edge ports since they directly connect to end stations.

Figure 15-8: RSTP Configuration Example



First, we restore both switches to their factory default configuration with the "switch defaults" command:

```
cpc1# switch defaults
cpc2# switch defaults
```

Because STP is the factory default, we need to configure both switches to run RSTP. We do that using the "span version" command:

```
cpc1# span version 2
cpc1# save
cpc1# switch reset


cpc2# span version 2
cpc2# save
cpc2# switch reset
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Next, we need to configure cpc1 to become a Root Bridge. The default Bridge Priority is 32768. By changing the priority of cpc1 to 4096, it will become the Root Bridge for our bridged network.

```
cpc1# span bridge priority 4096
```

We now need to adjust the Spanning Tree timers. We will adjust them on cpc1 since this switch operates as a Root Bridge for our network. We will set the Bridge_Hello_Time to 1 second, the Bridge_Forward_Delay to 4 seconds, and the Bridge_Max_Age to 6 seconds.

```
cpc1# span bridge hello 100
cpc1# span bridge delay 400
cpc1# span bridge maxage 600
```

Next, we will set ports 3-24 on both switches to operate as edge ports.

```
cpc1# span port edgeport 3-24 on
cpc2# span port edgeport 3-24 on
```

Finally, we need to save the configuration to NVRAM with the “save” command.

```
cpc1# save
cpc2# save
```

We do not need to reboot the switches since all Spanning Tree configuration parameters -- with the exception of “span version” and “span pathcost” -- take effect immediately. To verify our settings, we display the Spanning Tree configuration with the “span bridge show” command:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
cpc1# span bridge show

*****************************************************************
                    RSTP (version 2)
Spanning Tree (RSTP) is ENABLED  forceVersion = 2  RPC = 0
RootID: 100000c08c086084 BrID: 100000c08c086084 TC = NO  TCcnt = 0
MaxAge = 6, FwDel = 4, MesAge = 0, Hello = 1, Long Aging = 300
-----------------------------------------------------------------
 port portState   Role  Pcost Dcost Priority Edge P2P Ad/Pr ATime
-----------------------------------------------------------------
  1   Forwarding   D    19    0      128      NO   YES Y/Y   0/6
  2   Forwarding   D    19    0      128      NO   YES Y/Y   0/6
  3   Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  4   Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  5   Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  6   Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  7   Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  8   Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  9   Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  10  Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  11  Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  12  Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  13  Forwarding   D    19    0      128      YES  YES Y/Y   0/6
  14  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  15  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  16  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  17  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  18  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  19  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  20  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  21  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  22  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  23  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  24  Disabled     Di   19    0      128      YES  NO  N/Y   0/0
  25  Disabled     Di   4     0      128      NO   NO  N/Y   0/0
  26  Disabled     Di   4     0      128      NO   NO  N/Y   0/0

-----------------------------------------------------------------
D = Designated, A = Alternate, B = Backup, Di = Discarding
Ad/Pr = AdminState/ProtEnabled Atime = rcvdInfoWhile/MaxAge
```

We see that cpc1 is now a Root Bridge because the Root ID is the same as the Bridge ID. The Bridge ID is displayed in a hexadecimal format as an 8 byte value with the upper two bytes representing the Bridge Priority and the lower six bytes representing Bridge MAC address. The Bridge Priority is 0x1000, which is 4096 decimal, while the MAC address is 00c08c086084. We see that ports 3-24 are configured as Edge Ports, and that Ports 1-13 are Forwarding (Designated), while ports 14- are Disabled (Discarding) since these ports have no links.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Let's now examine the state of Spanning Tree on cpc2:

```
cpc2# span bridge show
```

```
*****************************************************************
                    RSTP (version 2)
Spanning Tree (RSTP) is ENABLED  forceVersion = 2  RPC = 19
RootID: 100000c08c086084 BrID: 800000c08c086128 TC = NO  TCcnt = 0
MaxAge = 6, FwDel = 4, MesAge = 0, Hello = 1, Long Aging = 300
-----------------------------------------------------------------
 port portState   Role  Pcost Dcost Priority Edge P2P Ad/Pr ATime
-----------------------------------------------------------------
  1   Forwarding   R    19    19     128      NO   YES Y/Y   3/6
  2   Forwarding   A    19    19     128      NO   YES Y/Y   3/6
  3   Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  4   Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  5   Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  6   Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  7   Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  8   Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  9   Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  10  Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  11  Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  12  Forwarding   D    19    19     128      YES  YES Y/Y   0/6
  13  Disabled     Di   19    19     128      YES  NO  N/Y   0/6
  14  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  15  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  16  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  17  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  18  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  19  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  20  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  21  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  22  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  23  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  24  Disabled     Di   19    19     128      YES  NO  N/Y   0/0
  25  Disabled     Di   4     19     128      NO   NO  N/Y   0/0
  26  Disabled     Di   4     19     128      NO   NO  N/Y   0/0

-----------------------------------------------------------------
D = Designated, A = Alternate, B = Backup, Di = Discarding
Ad/Pr = AdminState/ProtEnabled Atime = rcvdInfoWhile/MaxAge
```

Notice that the RootID and the BrID are different, indicating that this switch is not a Root Bridge. Also notice that the Root Path Cost (RPC) is set to 19 which is the cost of the path to the Root Bridge. Port 1 provides the connection to the Root Bridge (cpc1) and acts as a Root Port (R) while port 2 provides an alternative path to the Root Bridge and operates as an Alternate port (A). Ports 3-24 are configured as Edge Ports but only ports 1-12 have links. The last column (Atime) shows rcvdInfoWhle/MaxAge. The rcvdInfoWhile is a timer which starts at 3 x Bridge_Hello_Time and decrements by one every second if it does not receive a BPDU. This timer is being used as a "keep alive" timer to maintain an active connection with the upstream bridge. If no BPDUs are received within 3 x Bridge_Hello_Time, the switch concludes that its connection to the upstream bridge is lost. The Max Age is set to 6, which means that when a BPDU arrives on the switch port with a message age older than 6, it will be discarded.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

16

Link Aggregation

Overview

This chapter provides information on link aggregation on the CPC441x.

Note: *The examples provided throughout this section refer to the CPC440x (with 26 ports), but the implementation of Link Aggregation they illustrate is the same for the CPC441x.*

Link Aggregation allows two or more physical ports to be aggregated together forming a Link Aggregation Group, such that a MAC Client can treat the Link Aggregation Group as if it were a single link. Performance Technologies' Link Aggregation implementation fully conforms to the IEEE 802.3ad specification.

The key topics in this chapter include:

- "Link Aggregation Default Settings" on page 386
- "Architecture Overview" on page 388
- "Link Aggregation Configuration Examples" on page 394
- "Displaying Switch Configurations" on page 395

Benefits

By taking multiple LAN connections and treating them as a single, aggregated link, we can achieve several benefits:

- **Increased link capacity**. The total capacity of the aggregated link is the sum of the capacities of the individual links composing the aggregate.
- **Incremental capacity increase**. While LAN technology offers a variety of data rates, the available options are usually divided into an order-of-magnitude improvement; for example: 10 Mb/s, 100 Mb/s,

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

or 1000 Mb/s. Link aggregation can be used to fill the gaps when an intermediate performance level is more appropriate.

- **Higher link availability**. A properly designed link aggregation scheme will prevent the failure of any single component link from disrupting communication between the interconnected devices. For links requiring high availability, this feature may be more important than the link capacity increase. The loss of link within the aggregation reduces the available capacity but does not disrupt the communication entirely.

Link Aggregation Default Settings

The CPC441x consists of 24 10/100 Mb/s ports and 2 Gb/s ports, for a total of 26 ports (or, in the context of link aggregation, “aggregation ports”). There are also 26 aggregators, one for each aggregation port. The factory defaults are such that the CPC441x powers up with each aggregation port attached to its respective aggregator, i.e., port 1 is attached to aggregator 1, port 2 is attached to aggregator 2, etc. Although there are 26 aggregators, the underlying hardware allows for only 6 aggregation groups, with each group having up to eight aggregation ports.

Administrative Keys

Only ports with the same administrative key can be aggregated into a Link Aggregation Group. Following are the default administrative key assignments (“actor” refers to the local switch in a link aggregation group; “partner” refers to the remote switch):

- Ports 1-8 are assigned Actor’s Administrative Key of 1.
- Ports 9-16 are assigned Actor’s Administrative Key of 2.
- Ports 17-24 are assigned Actor’s Administrative Key of 3.
- Ports 25-26 are assigned Actor’s Administrative Key of 4.

Each port is also assigned a unique Partner’s administrative key, which is the same as its port number (port 1 has a Partner’s administrative key of 1; port 2 is key 2, etc.). This initial setting ensures that the CPC441x switch will not form an aggregation until it exchanges Link Aggregation Control Protocol Data Units (LACPDUs) with its protocol partner.

For example, if two CPC440xs (with 26 ports) with the same default settings are connected “back to back” (i.e., port 1 on both switches connected to each other, port 2 on both switches connected to each other, etc.), and Link Aggregation is enabled, then the two switches will initially be unable to form aggregations because all the ports (with the exception of port 1) have different actor and partner administrative keys. However, after an exchange of LACPDUs, the partner keys will update to match the actor keys, and four aggregation groups will be formed, per the default actor keys: ports 1-8 in the first group, ports 9-16 in the second group, ports 17-24 in the third group, and ports 25-26 in the fourth group. Notice that no additional configuration was necessary to form these link aggregation groups because we utilized the factory default settings. (See “Assign an Actor Key Value” on page 164.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Distribution Rules (“rtag”)

The CPC441x allows for distributing the Ethernet traffic among the aggregated links based on the Source and Destination MAC address and the Source and Destination IP address. The default rtag value assigned to all CPC441x ports is DestMAC. The distribution rule may be changed with the `lag config rtag` command. Following are the six rtag values and the distribution rule for each:

1. SrcMAC - indicates that packets are distributed based on the last three bits of the Source MAC address.
2. DestMAC - indicates that the packets are distributed based on the last three bits of the Destination MAC address.
3. SrcXORDestMAC - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination MAC address.
4. SrcIP - indicates that the packets are distributed based on the last three bits of the Source IP address.
5. DestIP - indicates that the packets are distributed based on the last three bits of the Destination IP address.
6. SrcXORDestIP - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination IP address.

Multiple packet items may be included as part of the packet distribution criteria. All packet items listed will be included as part of the distribution criteria. The selected items will be hashed to a port number within the aggregation. The hashing algorithm is proprietary and not configurable.Distribution rules are assigned to Trunk Groups rather than to ports or aggregators. When a group of aggregation ports select their aggregator, this aggregator becomes associated with a Trunk Group. The distribution rule assigned to the aggregator then becomes the Trunk Group’s distribution rule. For example, assume ports 1 and 2 have been assigned a distribution rule based on the SrcMAC, while ports 3 and 4 have been assigned a distribution rule based on DestIP. When these ports form an aggregation group, they select aggregator 1 as their aggregator, and they select the distribution rule based on aggregator 1’s distribution rule, which is SrcMAC. This distribution rule is then assigned to a Trunk Group, which represents aggregator 1. To avoid confusion, select the same distribution criteria for all ports that have the same administrative key.

If ports 1, 2, 3, and 4 are in the same aggregation group, we can assign them the same distribution rule (SrcMAC) with the following command:

```
# lag config rtag 1-4 SrcMAC
```

See “Assign Link Aggregation Distribution Criteria” on page 162.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

LACPDU Transmission Interval (“timeout”)

Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link allowing each system to reach agreement on the identity of the Link Aggregation Group to which the link belongs. Transmission of LACPDUs occurs either as a result of a periodic transmission, or as a result of changes to the Actor’s state information that need to be communicated to the Partner. The periodic transmission may occur at a Short timeout (1 sec.) or a Long timeout (30 sec.), which is determined by the Partner’s LACP_Timeout value. The CPC441x LACP_Timeout default value is set to a Long Timeout (30 sec.). See “Set Timeout” on page 166.

Architecture Overview

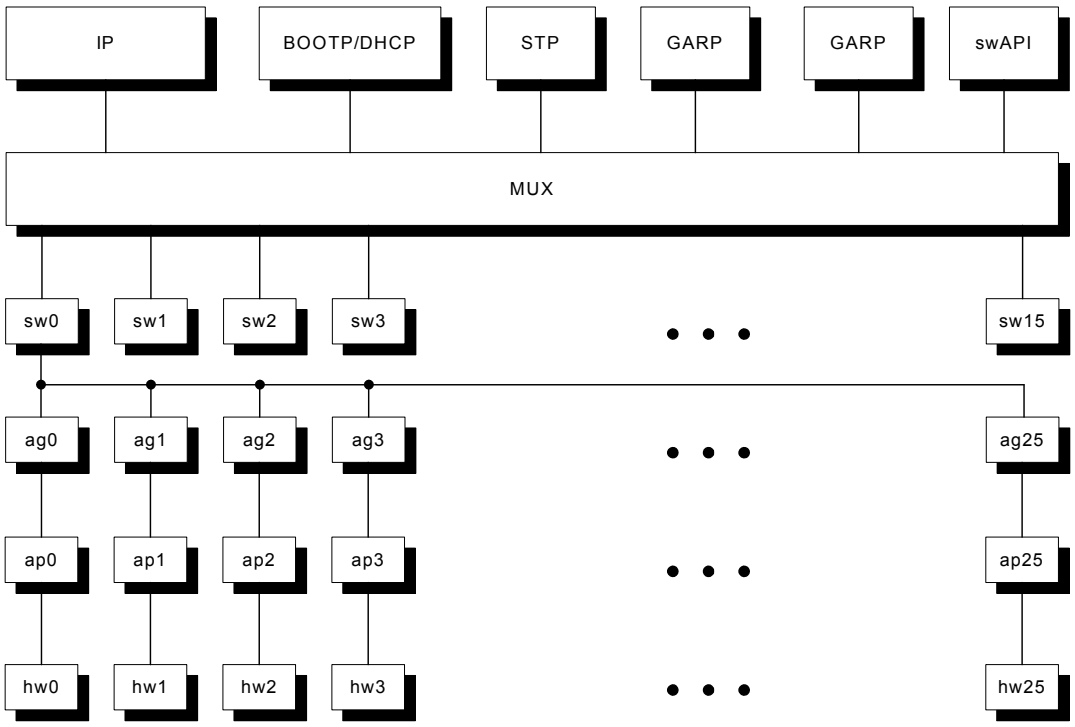
To support the IEEE 802.3ad Link Aggregation specification, CPC441x implements multiple layers of Network Device drivers, which include:

- Switch Network Drivers sw0 – sw15 represent the routing interfaces. In the CPC441x, the Switch Network Drivers represent IEEE 802.1Q VLANs.
- Aggregator Network Drivers ag0 – ag25 represent the IEEE 802.3ad Link Aggregation logical ports. The STP and GARP applications bind directly to these Aggregators, allowing the aggregation to participate in STP and GARP as a single entity.
- Aggregation Ports Network Drivers ap0 – ap25 represent the IEEE 802.3ad Link Aggregation physical ports or individual links in the Aggregation Group. The Aggregation Ports abstract the actual Hardware ND drivers in order to isolate the CPC441x core from the underlying switch hardware.
- Hardware Network Interface drivers hw0 – hw25 represent the physical hardware drivers.

This architecture is depicted in Figure 16-1: “CPC440x Architecture” on page 389 (for the CPC440x). (Figure 16-1 shows the default VLAN 1, ag0 – ag25, assigned to network interface sw0. In practice, this assignment would be made by the user. See the configuration example on page 390.)

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 16-1: CPC440x Architecture



The Aggregation layer abstracts the physical ports from applications such as VLAN, Spanning Tree, or GARP. For this reason, VLAN, Spanning Tree and GARP no longer see physical ports but instead operate on aggregators, sometimes referred to as “logical ports” (see Figure 16-1: “CPC440x Architecture”). When no aggregation exists, each aggregation port (ap) is attached to its respective aggregator (ag). When a group of ports join to form an aggregated link, only one of the aggregators becomes the aggregator for the entire group. The selection of an aggregator for the group is performed by the Link Aggregation algorithm and is beyond user control. However, the user can choose which ports will become members of the aggregated link by assigning the same administrative key to all ports in the group. Ports that have the same key, operate at full duplex, at the same speed, and are connected to a partner that conforms to the same rules, will form an aggregated link. Since it is beyond user control to select the aggregator for the group, all ports within the group need to be configured the same way. In particular, they must be assigned to the same VLAN.

To illustrate this further, consider two switches connected via ports 1-3. Both switches are configured to factory settings, which means that all ports belong to a default VLAN 1. We will change this configuration by assigning ports 1-8 to VLAN 2 and port 26 to VLAN 3. Next, we will assign a unique administrative key to ports 1-3 to allow them to form an aggregated link. Finally, we will enable link aggregation on the switch.

The following commands configure VLAN2 with ports 1-8 and VLAN 3 with port 26, all untagged:

```
# vlan create 2 vlan2 untagged=1-8
# vlan create 3 vlan3 untagged=26
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

To display current VLAN settings, execute a “vlan show” command:

```
# vlan show

CPC4400 VLAN TABLE
                                                    1         2
VLAN NAME                    VLAN ID
                                        123456789012345678901234
-------------------------------------------------------------------
Default                           1     UUUUUUUUUUUUUUUUUUUUUUUUUU
vlan2                             2     UUUUUUUU------------------
vlan3                             3     ------------------------U
```

Notice that all ports continue to belong to the default VLAN (VLAN 1). You may remove ports 1-8 and port 26 from the default VLAN by executing a “vlan remove” command:

```
# vlan remove 1 untagged=1-8,26
# vlan show

CPC4400 VLAN TABLE
                                                  1         2
VLAN NAME                    VLAN ID
                                        123456789012345678901234
-------------------------------------------------------------------
Default                           1     --------UUUUUUUUUUUUUUUU-
vlan2                             2     UUUUUUUU------------------
vlan3                             3     ------------------------U
```

We can now enable link aggregation on the switch. Remember that ports will not aggregate unless they are in the same VLAN. In our example this condition is met since ports 1-3 belong to VLAN 2. To allow ports 1-3 to aggregate, we must assign them the same administrative key. Furthermore, these ports must be connected to partners that fulfill the same conditions, i.e., that have the same administrative key and are in the same VLAN. (It is not required that the ports on both switches have the same key, only that all ports belonging to the same group on each switch have the same key.) The following commands assign a key value of 10 to ports 1-3 and enable link aggregation on the local switch.

```
# lag config actor akey 1-3 10
# lag enable on
```

To complete this example, we will assign network interfaces sw0 to VLAN 1, sw2 to VLAN 2, and sw3 to VLAN 3

```
# ip config sw0 172.16.1.1 255.255.240.0 1
# ip config sw2 172.16.16.1 255.255.240.0 2
# ip config sw3 172.16.32.1 255.255.240.0 3
```

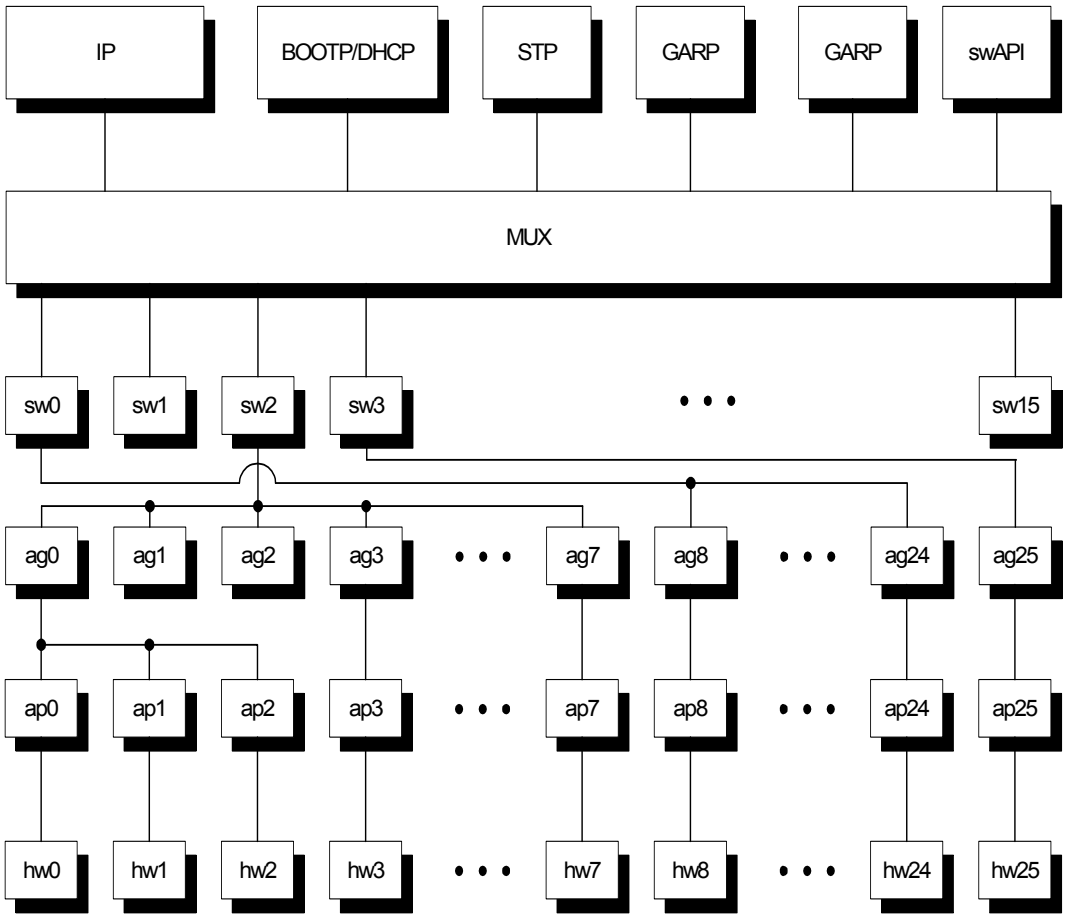

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

When referring to the architectural model depicted in Figure 16-2: “CPC440x with Ports 1-3 Aggregated” on page 391, we notice that ports 1-3 (ap0-ap2) are attached to aggregator1 (ag0). This is because ports 1-3 formed a single aggregated link. Aggregator 1 (ag0) has been chosen as the aggregator for the group. Ag1-ag2 are no longer connected to ap1-ap2 and, therefore, become isolated. Ports 4-8 (ap3-ap7) do not form an aggregation; that is, they continue to operate as individual ports and remain attached to their respective aggregators, ag3-ag7. Since we have placed ports 1-8 in VLAN 2 and configured sw2 as a network driver for VLAN 2, aggregators 1-8 (ag0-ag7) are now attached to sw2.

Port 26 (ap25) is also operating as an individual port, and remains connected to its own aggregator (ag25). Because we have assigned this port to VLAN 3 and configured sw3 to be a network driver for that VLAN, ag25 is attached to sw3.

The remaining ports, 9-25 (ap8-ap24), do not form an aggregation and are therefore attached to their respective aggregators. We have configured sw0 to be a network driver for VLAN 1, and so all aggregators in VLAN 1 are attached to sw0.

Figure 16-2: CPC440x with Ports 1-3 Aggregated

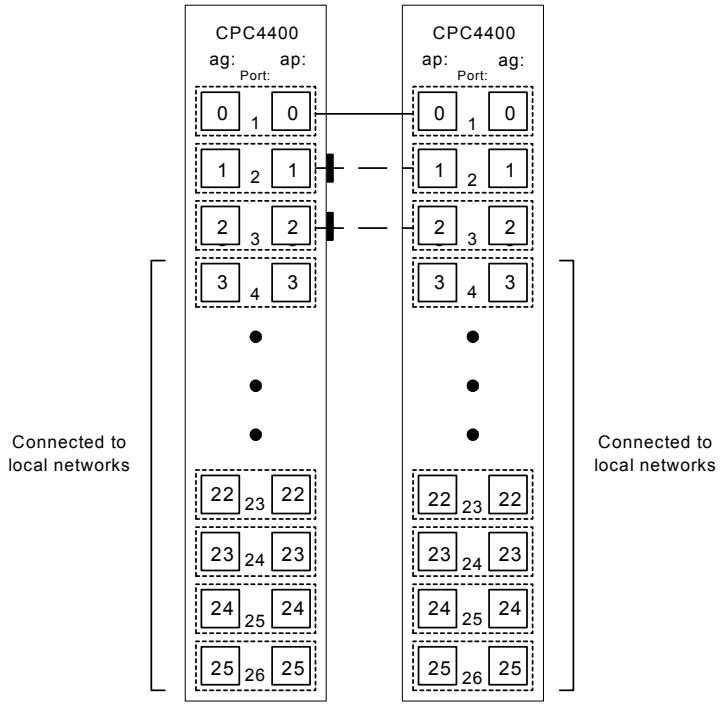


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Link Aggregation and Spanning Tree

Figure 16-3: “Ports in Blocking State” on page 392 represents two CPC440x switches connected via ports 1-3. Ports 4-26 on both switches are connected to various network segments. Each aggregation port is connected to its respective aggregator (i.e., each ap is connected to its ag). In such a case, the Spanning Tree Protocol (STP) would detect link on all the ports. It would also discover that ports 1, 2, and 3 are connected to the same Protocol Partner, and would block some ports so as to prevent loops. If the CPC440x on the right becomes a Root Bridge, then STP on the left switch will place ports 2 and 3 in the Blocking state, preventing any traffic from flowing through them.

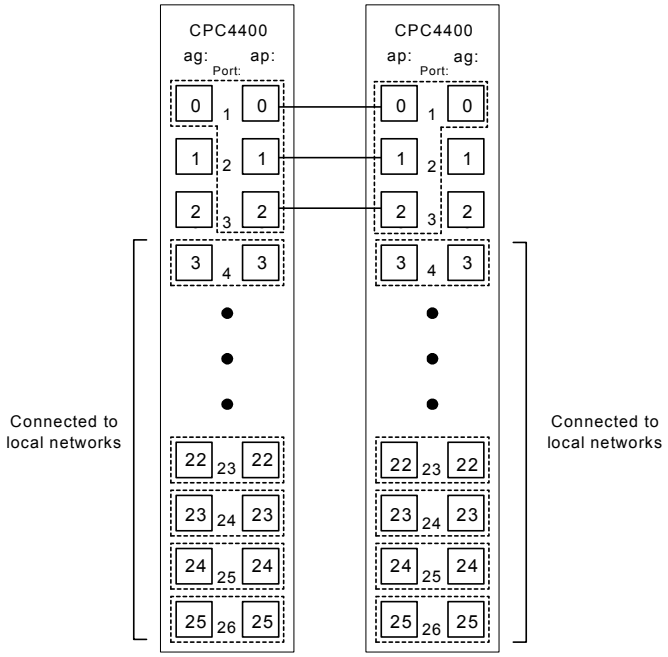
Figure 16-3: Ports in Blocking State



If we now form an aggregation link from ports 1-3, we have the situation diagrammed in Figure 16-2: “CPC440x with Ports 1-3 Aggregated” on page 391, and depicted below in Figure 16-4: “Ports 1 - 3 Aggregated” on page 393 Since ap0-ap2 are now connected to ag0, then ag1 and ag2 become isolated. Spanning Tree will treat them as if ports 2 and 3 (ag1 and ag2) have lost their links. The ag0 will be placed in a Forwarding state because, from Spanning Tree’s perspective, this is the only port that connects both switches. Since ap0-ap2 are attached to ag0, their states will also be Forwarding. There will be no loop since these ports are treated as one link. Traffic between both CPC440xs will be distributed between these three ports based on the rtag distribution criteria. Should any of the three links break, the IEEE 802.3ad Link Aggregation software will automatically notice the fact and continue to use the two remaining links to distribute the traffic between the two switches.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 16-4: Ports 1 - 3 Aggregated



The benefits of aggregating ports 1-3 are now clear: we have boosted the throughput between the two switches from 100 Mb/s to 300 Mb/s; a loss of a link will no longer cause the STP to reconfigure; the STP will continue to see ag0 as having an active link so long as at least one of the aggregation ports connected to ag0 maintains an active link.

Note: *When examining the STP port states, remember that you are observing the states of the Aggregators (ags) as opposed to the Aggregation Ports (aps). (Use the* `lag show` *commands to view the Link Aggregation status.) Likewise, STP, GARP and VLAN applications deal with the Aggregators rather than the Aggregation Ports.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Link Aggregation Configuration Examples

For our example, we want to connect two CPC440xs via ports 1-3 and port 10, and we want to create an aggregated link using those ports. We also want the distribution criteria to be based on the Destination IP address, and the periodic transmission on both switches to be set to Short timeout (1 sec.).

To accomplish this, we need to assign the same key to all the ports in the group on both switches. We then need to assign a distribution rule of DestIP for ports 1-3 and 10, and change the timeout to SHORT timeout. The following commands for both switches will achieve the desired configuration:

Switch 1:

```
Switch1# lag enable on
Switch1# lag config actor akey 1-3 10
Switch1# lag config actor akey 10 10
Switch1# lag config rtag 1-3 DestIP
Switch1# lag config rtag 10 DestIP
Switch1# lag config actor timeout 1-3 short
Switch1# lag config actor timeout 10 short
```

Switch 2:

```
Switch2# lag enable on
Switch2# lag config actor akey 1-3  10
Switch2# lag config actor akey 10 10
Switch2# lag config rtag 1-3 DestIP
Switch2# lag config rtag 10 DestIP
Switch2# lag config actor timeout 1-3 short
Switch2# lag config actor timeout 10 short
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Displaying Switch Configurations

Now that we understand the relation between different Network Driver Layers, we can display the switch configuration to see Link Aggregation's effect on Spanning Tree, and to confirm that the proper aggregation has taken place.

Again, we start with two CPC440xs connected via ports 1-3 (Figure 16-3: "Ports in Blocking State" on page 392). Let's first look at the Spanning Tree before we enable Link Aggregation on both switches. Display the Spanning Tree configuration for the switch on the left in Figure 16-3: "Ports in Blocking State" with the following command:

```
cpc1#: span bridge show
```

Figure 16-5: Spanning Tree Configuration on Switch 1

```
****************************************************************
RootID: 8000000331010002 BridgeID: 800000c08c086004  RPC = 19
Spanning Tree ENABLED    fastUplink DISABLED  Top. Change = 1
Max Age = 20, Forw. Del = 15, Hold Time = 1
----------------------------------------------------------------
port portState   state  Pcost Dcost Priority portF   Protocol ATime
----------------------------------------------------------------
 1   FORWARDING    R    19    0     128      OFF     Enabled  A 1
 2   BLOCKING      B    19    0     128      OFF     Enabled  A 1
 3   BLOCKING      B    19    0     128      OFF     Enabled  A 1
 4   DISABLED      D    19    19    128      OFF     Enabled  N
 5   DISABLED      D    19    19    128      OFF     Enabled  N
 6   DISABLED      D    19    19    128      OFF     Enabled  N
 7   DISABLED      D    19    19    128      OFF     Enabled  N
 8   DISABLED      D    19    19    128      OFF     Enabled  N
 9   DISABLED      D    10    19    128      OFF     Enabled  N
 10  DISABLED      D    10    19    128      OFF     Enabled  N
 11  DISABLED      D    10    19    128      OFF     Enabled  N
 12  DISABLED      D    10    19    128      OFF     Enabled  N
 13  DISABLED      D    10    19    128      OFF     Enabled  N
 14  DISABLED      D    10    19    128      OFF     Enabled  N
 15  DISABLED      D    10    19    128      OFF     Enabled  N
 16  DISABLED      D    10    19    128      OFF     Enabled  N
 17  DISABLED      D    10    19    128      OFF     Enabled  N
 18  DISABLED      D    10    19    128      OFF     Enabled  N
 19  FORWARDING    D    19    19    128      OFF     Enabled  N
 20  DISABLED      D    10    19    128      OFF     Enabled  N
 21  FORWARDING    D    19    19    128      OFF     Enabled  N
 22  DISABLED      D    10    19    128      OFF     Enabled  N
 23  FORWARDING    D    100   19    128      OFF     Enabled  N
 24  DISABLED      D    10    19    128      OFF     Enabled  N
 25  DISABLED      D    10    19    128      OFF     Enabled  N
 26  DISABLED      D    10    19    128      OFF     Enabled  N
----------------------------------------------------------------
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Notice that cpc1 is not a Root Bridge. Its Bridge ID is 800000c08c086004, while the Root ID is 8000000331010002 (this is a Bridge ID of cpc2, the switch on the right in Figure 16-3: “Ports in Blocking State” on page 392). Also notice that port 1 is in the Forwarding state, while ports 2 and 3 are Blocked. The STP blocked these ports because they provide redundant paths to cpc2, and not blocking them would result in loops. Ports 19, 21 and 23 are connected to three different network segments and are in Forwarding states.

We can now examine the STP state on the second switch, cpc2, using the same command:

```
cpc2# span bridge show
```

Figure 16-6: Spanning Tree Configuration on Switch 2

```
*****************************************************************
RootID: 8000000331010002 BridgeID: 8000000331010002  RPC = 0
Spanning Tree ENABLED    fastUplink DISABLED  Top. Change = 0
Max Age = 20, Forw. Del = 15, Hold Time = 1
-----------------------------------------------------------------
port portState   state  Pcost Dcost Priority portF   Protocol ATime
-----------------------------------------------------------------
 1   FORWARDING    D    19    0     128      OFF     Enabled  N
 2   FORWARDING    D    19    0     128      OFF     Enabled  N
 3   FORWARDING    D    19    0     128      OFF     Enabled  N
 4   DISABLED      D    10    0     128      OFF     Enabled  N
 5   DISABLED      D    10    0     128      OFF     Enabled  N
 6   DISABLED      D    10    0     128      OFF     Enabled  N
 7   DISABLED      D    10    0     128      OFF     Enabled  N
 8   DISABLED      D    10    0     128      OFF     Enabled  N
 9   DISABLED      D    10    0     128      OFF     Enabled  N
 10  DISABLED      D    10    0     128      OFF     Enabled  N
 11  DISABLED      D    10    0     128      OFF     Enabled  N
 12  DISABLED      D    10    0     128      OFF     Enabled  N
 13  DISABLED      D    10    0     128      OFF     Enabled  N
 14  DISABLED      D    10    0     128      OFF     Enabled  N
 15  FORWARDING    D    19    0     128      OFF     Enabled  N
 16  DISABLED      D    10    0     128      OFF     Enabled  N
 17  DISABLED      D    10    0     128      OFF     Enabled  N
 18  DISABLED      D    10    0     128      OFF     Enabled  N
 19  FORWARDING    D    19    0     128      OFF     Enabled  N
 20  DISABLED      D    10    0     128      OFF     Enabled  N
 21  FORWARDING    D    100   0     128      OFF     Enabled  N
 22  DISABLED      D    10    0     128      OFF     Enabled  N
 23  FORWARDING    D    100   0     128      OFF     Enabled  N
 24  DISABLED      D    10    0     128      OFF     Enabled  N
 25  DISABLED      D    10    0     128      OFF     Enabled  N
 26  DISABLED      D    10    0     128      OFF     Enabled  N
-----------------------------------------------------------------
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

We see from this configuration that cpc2 is the Root Bridge, since its Bridge ID and the Root ID are the same. Because cpc2 is the Root Bridge, it did not need to block ports 2 and 3 (cpc1 blocked them). We also notice that on cpc2, ports 15, 19, 21 and 23 are connected to different network segments and are set to a Forwarding state.

Before we enable Link Aggregation on both switches, we can verify that it is not currently enabled by executing the “lag enable” command on both switches. Remember that if no arguments are provided, the “lag enable” displays the current state of the Link Aggregation:

```
cpc1# lag enable
cpc1# off
cpc2# lag enable
cpc2# off
```

To enable Link Aggregation on both switches, use the “lag enable on” command:

```
cpc1# lag enable on
cpc2# lag enable on
```

Remember that, by default, ports 1-8 are assigned an administrative key equal to 1, ports 9-16 have a key value set to 2, ports 17-24 have a key set to 3, and the two gigabit ports 25-26 have a key set to 4. If we do not change the key, ports 1-3 can automatically aggregate since the local value of their keys is the same. In other words, the “lag enable on” command is all that’s needed to aggregate ports 1-3 on both switches. We can change the key value with the “lag actor config akey” command, but in this example the default keys make that unnecessary.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Now that we have aggregated ports 1-3, we can examine Spanning Tree on both switches with the “span bridge show” command:

```
cpc1# span bridge show
```

Figure 16-7: Spanning Tree after Link Aggregation, Switch 1

```
*****************************************************************
RootID: 8000000331010002 BridgeID: 800000c08c086004  RPC = 19
Spanning Tree ENABLED    fastUplink DISABLED  Top. Change = 1
Max Age = 20, Forw. Del = 15, Hold Time = 1
-----------------------------------------------------------------
port portState   state  Pcost Dcost Priority portF   Protocol ATime
-----------------------------------------------------------------
 1   FORWARDING    R    19    0     128      OFF     Enabled  A 1
 2   DISABLED      D    19    19    128      OFF     Enabled  N
 3   DISABLED      D    19    19    128      OFF     Enabled  N
 4   DISABLED      D    19    19    128      OFF     Enabled  N
 5   DISABLED      D    19    19    128      OFF     Enabled  N
 6   DISABLED      D    19    19    128      OFF     Enabled  N
 7   DISABLED      D    19    19    128      OFF     Enabled  N
 8   DISABLED      D    19    19    128      OFF     Enabled  N
 9   DISABLED      D    10    19    128      OFF     Enabled  N
 10  DISABLED      D    10    19    128      OFF     Enabled  N
 11  DISABLED      D    10    19    128      OFF     Enabled  N
 12  DISABLED      D    10    19    128      OFF     Enabled  N
 13  DISABLED      D    10    19    128      OFF     Enabled  N
 14  DISABLED      D    10    19    128      OFF     Enabled  N
 15  DISABLED      D    10    19    128      OFF     Enabled  N
 16  DISABLED      D    10    19    128      OFF     Enabled  N
 17  DISABLED      D    10    19    128      OFF     Enabled  N
 18  DISABLED      D    10    19    128      OFF     Enabled  N
 19  FORWARDING    D    19    19    128      OFF     Enabled  N
 20  DISABLED      D    10    19    128      OFF     Enabled  N
 21  FORWARDING    D    19    19    128      OFF     Enabled  N
 22  DISABLED      D    10    19    128      OFF     Enabled  N
 23  FORWARDING    D    100   19    128      OFF     Enabled  N
 24  DISABLED      D    10    19    128      OFF     Enabled  N
 25  DISABLED      D    10    19    128      OFF     Enabled  N
 26  DISABLED      D    10    19    128      OFF     Enabled  N
-----------------------------------------------------------------
```

Ports 2 and 3 on cpc1 are now disabled. To understand why, See Figure 16-4: “Ports 1 - 3 Aggregated” on page 393. Remember that STP shows the state of the Aggregators rather than the Aggregation Ports. In our example, ports ap0-ap2 (ports 1-3) created one aggregation group and attached to Aggregator 1 (ag0). Aggregators 2 and 3 (ag1 and ag2) are no longer attached to aggregation ports -- they have become isolated. From Spanning Tree’s perspective, it appears that ports 2 and 3 have lost their links. The physical ports obviously have not lost their links, and are connected to aggregator 1. When Spanning Tree set aggregator 1 to a Forwarding state, all physical ports attached to this aggregator automatically became forwarding as well. In other words, the aggregation ports share the Spanning Tree State of their aggregator. In our case, aggregation ports 1-3 are attached to aggregator 1 and therefore share its Spanning Tree state.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Before we examine the state of the aggregation, let's look at the state of Spanning Tree on cpc2:

```
cpc2# span bridge show
```

Figure 16-8: Spanning Tree after Link Aggregation, Switch 2

```
**************************************************************
RootID: 8000000331010002 BridgeID: 8000000331010002  RPC = 0
Spanning Tree ENABLED    fastUplink DISABLED  Top. Change = 1
Max Age = 20, Forw. Del = 15, Hold Time = 1
--------------------------------------------------------------
port portState   state  Pcost Dcost Priority portF   Protocol ATime
--------------------------------------------------------------
 1   FORWARDING    D    19    0     128      OFF     Enabled  N
 2   DISABLED      D    19    0     128      OFF     Enabled  N
 3   DISABLED      D    19    0     128      OFF     Enabled  N
 4   DISABLED      D    10    0     128      OFF     Enabled  N
 5   DISABLED      D    10    0     128      OFF     Enabled  N
 6   DISABLED      D    10    0     128      OFF     Enabled  N
 7   DISABLED      D    10    0     128      OFF     Enabled  N
 8   DISABLED      D    10    0     128      OFF     Enabled  N
 9   DISABLED      D    10    0     128      OFF     Enabled  N
 10  DISABLED      D    10    0     128      OFF     Enabled  N
 11  DISABLED      D    10    0     128      OFF     Enabled  N
 12  DISABLED      D    10    0     128      OFF     Enabled  N
 13  DISABLED      D    10    0     128      OFF     Enabled  N
 14  DISABLED      D    10    0     128      OFF     Enabled  N
 15  FORWARDING    D    19    0     128      OFF     Enabled  N
 16  DISABLED      D    10    0     128      OFF     Enabled  N
 17  DISABLED      D    10    0     128      OFF     Enabled  N
 18  DISABLED      D    10    0     128      OFF     Enabled  N
 19  FORWARDING    D    19    0     128      OFF     Enabled  N
 20  DISABLED      D    10    0     128      OFF     Enabled  N
 21  FORWARDING    D    100   0     128      OFF     Enabled  N
 22  DISABLED      D    10    0     128      OFF     Enabled  N
 23  FORWARDING    D    100   0     128      OFF     Enabled  N
 24  DISABLED      D    10    0     128      OFF     Enabled  N
 25  DISABLED      D    10    0     128      OFF     Enabled  N
 26  DISABLED      D    10    0     128      OFF     Enabled  N
--------------------------------------------------------------
```

Again we see that the isolation of aggregators 2 and 3 has resulted in Spanning Tree disabling them (remember that Spanning Tree shows the state of the aggregators rather than the physical ports). Aggregation ports 1-3 share the Spanning Tree state of aggregator 1 and are in a Forwarding state.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

We now wish to verify that ports 1-3 are indeed aggregated. There are several commands we can use. Let's start with the "lag show states" command, which displays the states of the Link Aggregation State Machines.

```
cpc1# lag show states
```

Figure 16-9: LACP State Machines, Switch 1

```
*****************************************************************
             LACP State Machines: ver 01  LAC ENABLED
-----------------------------------------------------------------
Port Receive    Transmit      Selection  Mux        LACP Ag CD
-----------------------------------------------------------------
01   CURRENT    PERIODIC_TX   SELECTED   COL_DISTR  YES  01 1
02   CURRENT    PERIODIC_TX   SELECTED   COL_DISTR  YES  01 1
03   CURRENT    PERIODIC_TX   SELECTED   COL_DISTR  YES  01 1
04   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   04 0
05   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   05 0
06   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   06 0
07   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   07 0
08   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   08 0
09   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   09 0
10   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   10 0
11   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   11 0
12   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   12 0
13   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   13 0
14   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   14 0
15   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   15 0
16   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   16 0
17   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   17 0
18   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   18 0
19   LACP_DISAB NO_PERIODIC   SELECTED   COL_DISTR  NO   19 1
20   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   20 0
21   LACP_DISAB NO_PERIODIC   SELECTED   COL_DISTR  NO   21 1
22   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   22 0
23   LACP_DISAB NO_PERIODIC   SELECTED   COL_DISTR  NO   23 1
24   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   24 0
25   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   25 0
26   P_DISABLED NO_PERIODIC   SELECTED   ATTACHED   NO   26 0
-----------------------------------------------------------------
```

We notice that ports 1-3 are in the CURRENT states, which means that they periodically receive Link Aggregation Control Protocol Data Units (LACPDUs) from their protocol partner. We also notice that LACP protocol is enabled on all three ports and that all three ports chose aggregator 1 ("Ag = 01") as their aggregator. The MUX machine is in the COL_DIST (collecting-distributing) state, indicating that these ports actively participate in data transfer (i.e., packet reception and transmission is enabled on these ports).

Ports 19, 21, and 23 do not run the LACP protocols and the Receive State Machine is in a LACP_DISABLED state. In order for the LACP to be activated on a port, it needs to run in Full Duplex mode. According to the IEEE802.3ad, ports that run in Half Duplex mode cannot form an aggregation. We can verify that this is the case by executing a "lag show port" command:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
cpc1# lag show port
```

Figure 16-10: LAC Port Information, Switch 1

```
*************************************************************************
                          LAC Port Information
-------------------------------------------------------------------------
P# PP# NTT MAC               Key Pri State     PState    Move Lnk  Dpx  Spd
-------------------------------------------------------------------------
01 001 NO  00:c0:8c:08:60:52 001 128 1011 1100 1011 1100 NO   Up   Full 100
02 002 NO  00:c0:8c:08:60:d2 001 128 1011 1100 1011 1100 NO   Up   Full 100
03 003 NO  00:c0:8c:08:60:32 001 128 1011 1100 1011 1100 NO   Up   Full 100
04 004 NO  00:c0:8c:08:60:b2 001 128 1011 0010 0000 1110 NO   Dwn  ?    100
05 005 NO  00:c0:8c:08:60:72 001 128 1011 0010 0000 1110 NO   Dwn  ?    100
06 006 NO  00:c0:8c:08:60:f2 001 128 1011 0010 0000 1110 NO   Dwn  ?    100
07 007 NO  00:c0:8c:08:60:0a 001 128 1011 0010 0000 1110 NO   Dwn  ?    100
08 008 NO  00:c0:8c:08:60:8a 001 128 1011 0010 0000 1110 NO   Dwn  ?    100
09 009 NO  00:c0:8c:08:60:4a 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
10 010 NO  00:c0:8c:08:60:ca 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
11 011 NO  00:c0:8c:08:60:2a 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
12 012 NO  00:c0:8c:08:60:aa 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
13 013 NO  00:c0:8c:08:60:6a 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
14 014 NO  00:c0:8c:08:60:ea 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
15 015 NO  00:c0:8c:08:60:1a 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
16 016 NO  00:c0:8c:08:60:9a 002 128 1011 0010 0000 1110 NO   Dwn  ?    100
17 017 NO  00:c0:8c:08:60:5a 003 128 1011 0010 0000 1110 NO   Dwn  ?    100
18 018 NO  00:c0:8c:08:60:da 003 128 1011 0010 0000 1110 NO   Dwn  ?    100
19 019 NO  00:c0:8c:08:60:3a 003 128 1011 1110 0001 1110 NO   Up   Half 100
20 020 NO  00:c0:8c:08:60:ba 003 128 1011 0010 0000 1110 NO   Dwn  ?    100
21 021 NO  00:c0:8c:08:60:7a 003 128 1011 1110 0001 1110 NO   Up   Half 100
22 022 NO  00:c0:8c:08:60:fa 003 128 1011 0010 0000 1110 NO   Dwn  ?    100
23 023 NO  00:c0:8c:08:60:06 003 128 1011 1110 0001 1110 NO   Up   Half 10
24 024 NO  00:c0:8c:08:60:86 003 128 1011 0010 0000 1110 NO   Dwn  ?    100
25 025 NO  00:c0:8c:08:60:46 004 128 1011 0010 0000 1110 NO   Dwn  ?    1000
26 026 NO  00:c0:8c:08:60:c6 004 128 1011 0010 0000 1110 NO   Dwn  ?    1000
-------------------------------------------------------------------------
State = Activity Timeout Agg. Sync. Coll. Dist. Def. Exp.
-------------------------------------------------------------------------
```

Here we notice that ports 19 and 21 operate in 100 Mb/s Half Duplex mode and that port 23 operates in 10 Mb/s Half Duplex mode, which explains why these ports are in an LACP_DISABLED state. We also notice that the remaining ports (4-18, 20, 22, 24-26) are down, which explains why their Receive State Machines are in a P_DISABLED (port disabled) state.

The “lag show port” command also allows us to examine the Actor and Partner States. We see in our example that both the Actor and Partner states for ports 1-3 are the same: 1011 1100. These 8 bits represent the following:

- Activity (“1”): Both systems are active (0 = inactive).
- Timeout (“0”): The current_while_timer is set to Long_Timeout_Time (30 seconds) (1 = short timer, 1 second).
- Aggregation (“1”): Ports 1-3 are in aggregation (0 = not aggregated).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- Synchronization (“1”): Ports 1-3 are “in sync,” i.e., both systems’ information is in agreement (0 = not in sync).
- Collecting (“1”): Ports 1-3 are in collecting mode (0 = not in collecting mode).
- Distributing (“1”): Ports 1-3 are in distribution mode (0 = not in distributing mode).
- Default (“0”): Ports 1-3 are not in defaulted state, (1 = defaulted).
- Expired (“0”): Ports 1-3 are not in expired state (1 = expired). Ports enter expired state when they do not receive LACPDUs before the current_while_timer expires. When this happens, the Receive state machine changes the Timeout value to a short timeout and waits for an additional 3 seconds. If LACPDUs are still not received, the port enters the defaulted state, and protocol information previously received from the protocol partner is replaced with the administrative defaults.

We also notice that all 26 ports retain their factory default local (actor) key values: ports 1-8 are set to 1, ports 9-16 are set to 2, ports 17-24 are set to 3, and ports 25-26 are set to 4. You can change the key value with the “lag config actor akey” command.

Let’s now execute the “lag show agg_port” command on the cpc1:

```
cpc1# lag show agg_port
```

Figure 16-11: LAC Aggregator Port Information, Switch 1

```
*****************************************************************
                  LAC Aggregator Port Information
-----------------------------------------------------------------
P# AKey PKey Loop Ind  APort Pbits                         Ports
-----------------------------------------------------------------
01 0001 0001 NO   NO   0001  00 00000000 00000000 00000111  1,3,2,
02 0001 0001 NO   NO   0001  00 00000000 00000000 00000000  1,3,2,
03 0001 0001 NO   NO   0001  00 00000000 00000000 00000000  1,3,2,
04 0001 0004 NO   YES  0004  00 00000000 00000000 00000000  4,
05 0001 0005 NO   YES  0005  00 00000000 00000000 00000000  5,
06 0001 0006 NO   YES  0006  00 00000000 00000000 00000000  6,
07 0001 0007 NO   YES  0007  00 00000000 00000000 00000000  7,
08 0001 0008 NO   YES  0008  00 00000000 00000000 00000000  8,
09 0002 0009 NO   YES  0009  00 00000000 00000000 00000000  9,
10 0002 0010 NO   YES  0010  00 00000000 00000000 00000000  10,
11 0002 0011 NO   YES  0011  00 00000000 00000000 00000000  11,
12 0002 0012 NO   YES  0012  00 00000000 00000000 00000000  12,
13 0002 0013 NO   YES  0013  00 00000000 00000000 00000000  13,
14 0002 0014 NO   YES  0014  00 00000000 00000000 00000000  14,
15 0002 0015 NO   YES  0015  00 00000000 00000000 00000000  15,
16 0002 0016 NO   YES  0016  00 00000000 00000000 00000000  16,
17 0003 0017 NO   YES  0017  00 00000000 00000000 00000000  17,
18 0003 0018 NO   YES  0018  00 00000000 00000000 00000000  18,
19 0003 0019 NO   YES  0019  00 00000100 00000000 00000000  19,
20 0003 0020 NO   YES  0020  00 00000000 00000000 00000000  20,
21 0003 0021 NO   YES  0021  00 00010000 00000000 00000000  21,
22 0003 0022 NO   YES  0022  00 00000000 00000000 00000000  22,
23 0003 0023 NO   YES  0023  00 01000000 00000000 00000000  23,
24 0003 0024 NO   YES  0024  00 00000000 00000000 00000000  24,
25 0004 0025 NO   YES  0025  00 00000000 00000000 00000000  25,
26 0004 0026 NO   YES  0026  00 00000000 00000000 00000000  26,
-----------------------------------------------------------------
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Here we see that ports 1-3 form an aggregation group but only port 1's mask (Pbits) shows all the ports as active. This means that port 1's aggregator contains the bit mask, which includes all aggregated ports, and this bit mask is programmed into the CPC440x hardware. We see that ports 19, 21 and 23 have their Pbits set, which means that they also are capable of moving traffic, although they do not form an aggregation. We also notice that ports 1-3 are not individual, meaning that these ports are capable of forming an aggregation. The rest of the ports are set as individual by the Link Aggregation State Machines because they either operate at half duplex or are down.

We can now examine Link Aggregation statistics using the "lag show stats" command:

```
cpc1# lag show stats
```

Figure 16-12: LAC Port Statistics, Switch 1

```
********************************************************************************
                                LAC Port Statistics
--------------------------------------------------------------------------------
P#  PL TxPDU  RxPDU  RxIllg RxUnkn RxMrk  RxMrs  hold moved  ChangeCt  TransCt
--------------------------------------------------------------------------------
01  UU 000014 000014 000000 000000 000000 000000 0001 0000   00000002  00000002
02  UU 000014 000014 000000 000000 000000 000000 0001 0000   00000002  00000002
03  UU 000014 000014 000000 000000 000000 000000 0001 0000   00000002  00000002
04  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
05  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
06  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
07  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
08  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
09  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
10  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
11  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
12  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
13  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
14  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
15  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
16  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
17  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
18  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
19  UD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
20  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
21  UD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
22  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
23  UD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
24  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
25  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
26  DD 000000 000000 000000 000000 000000 000000 0000 0000   00000000  00000000
--------------------------------------------------------------------------------
```

We notice that only ports 1-3 transmit and receive the LACPDUs.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Finally we can examine the Link Aggregation Identifiers on all ports:

```
cpc1# lag show ID
```

Figure 16-13: Link Aggregation Identifiers, Switch 1

```
*******************************************************************************
                        [(actor LAG ID), (partner LAG ID)]
-------------------------------------------------------------------------------
P# A# [(Prio,actor MAC address,key ,pr,P # ), (Prio,partn MAC address,key ,pr,P # ])
-------------------------------------------------------------------------------
01 01 [(8000,00-c0-8c-08-60-04,0001,00,0000), (8000,00-03-31-01-00-02,0001,00,0000)]
02 01 [(8000,00-c0-8c-08-60-04,0001,00,0000), (8000,00-03-31-01-00-02,0001,00,0000)]
03 01 [(8000,00-c0-8c-08-60-04,0001,00,0000), (8000,00-03-31-01-00-02,0001,00,0000)]
04 04 [(8000,00-c0-8c-08-60-04,0001,80,0004), (8000,00-00-00-00-00-00,0004,80,0004)]
05 05 [(8000,00-c0-8c-08-60-04,0001,80,0005), (8000,00-00-00-00-00-00,0005,80,0005)]
06 06 [(8000,00-c0-8c-08-60-04,0001,80,0006), (8000,00-00-00-00-00-00,0006,80,0006)]
07 07 [(8000,00-c0-8c-08-60-04,0001,80,0007), (8000,00-00-00-00-00-00,0007,80,0007)]
08 08 [(8000,00-c0-8c-08-60-04,0001,80,0008), (8000,00-00-00-00-00-00,0008,80,0008)]
09 09 [(8000,00-c0-8c-08-60-04,0002,80,0009), (8000,00-00-00-00-00-00,0009,80,0009)]
10 10 [(8000,00-c0-8c-08-60-04,0002,80,000a), (8000,00-00-00-00-00-00,000a,80,000a)]
11 11 [(8000,00-c0-8c-08-60-04,0002,80,000b), (8000,00-00-00-00-00-00,000b,80,000b)]
12 12 [(8000,00-c0-8c-08-60-04,0002,80,000c), (8000,00-00-00-00-00-00,000c,80,000c)]
13 13 [(8000,00-c0-8c-08-60-04,0002,80,000d), (8000,00-00-00-00-00-00,000d,80,000d)]
14 14 [(8000,00-c0-8c-08-60-04,0002,80,000e), (8000,00-00-00-00-00-00,000e,80,000e)]
15 15 [(8000,00-c0-8c-08-60-04,0002,80,000f), (8000,00-00-00-00-00-00,000f,80,000f)]
16 16 [(8000,00-c0-8c-08-60-04,0002,80,0010), (8000,00-00-00-00-00-00,0010,80,0010)]
17 17 [(8000,00-c0-8c-08-60-04,0003,80,0011), (8000,00-00-00-00-00-00,0011,80,0011)]
18 18 [(8000,00-c0-8c-08-60-04,0003,80,0012), (8000,00-00-00-00-00-00,0012,80,0012)]
19 19 [(8000,00-c0-8c-08-60-04,0003,80,0013), (8000,00-00-00-00-00-00,0013,80,0013)]
20 20 [(8000,00-c0-8c-08-60-04,0003,80,0014), (8000,00-00-00-00-00-00,0014,80,0014)]
21 21 [(8000,00-c0-8c-08-60-04,0003,80,0015), (8000,00-00-00-00-00-00,0015,80,0015)]
22 22 [(8000,00-c0-8c-08-60-04,0003,80,0016), (8000,00-00-00-00-00-00,0016,80,0016)]
23 23 [(8000,00-c0-8c-08-60-04,0003,80,0017), (8000,00-00-00-00-00-00,0017,80,0017)]
24 24 [(8000,00-c0-8c-08-60-04,0003,80,0018), (8000,00-00-00-00-00-00,0018,80,0018)]
25 25 [(8000,00-c0-8c-08-60-04,0004,80,0019), (8000,00-00-00-00-00-00,0019,80,0019)]
26 26 [(8000,00-c0-8c-08-60-04,0004,80,001a), (8000,00-00-00-00-00-00,001a,80,001a)]
-------------------------------------------------------------------------------
```

We notice that, with the exception of ports 1-3, all ports have their port number included in their LAG ID while ports 1-3 have their port number set to 0. This is an indication that only ports 1-3 form an aggregation group. Furthermore, we see that all ports with the exception of ports 1-3 have their partner's MAC address set to 00-00-00-00-00-00. This is a factory default. Ports 1-3 exchanged the LACPDUs and communicated their real MAC addresses. Notice that the local (actor's) MAC address is the same on all the ports. This is a System MAC address which represents the CPC440x switch as opposed to the individual ports. You may examine the port MAC addresses with the "lag show port" command and the aggregator MAC addresses with the "lag show agg" command.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

17

Multicast Filtering

Overview

The CPC441x supports static and dynamic multicast filtering. Multicast filtering allows the user to restrict the propagation of frames destined for a group of recipients to only those ports that provide a path to devices in that group. This functionality is supported with three mechanisms: Static Multicast, GARP Multicast Registration Protocol (GMRP), and Internet Group Management Protocol (IGMP) Snooping. Each of these mechanisms may be used independently or in conjunction with the others.

Up to twenty Multicast Groups may be configured at a time on the switch if GMRP and GVRP are enabled. If both of these features are disabled, then up to 255 multicast groups can be configured. The Filtering Database has 32K entries. Any entry may be used for a unicast or a multicast address.

The key topics in this chapter include:

- "Static Multicast Groups" on page 405
- "GMRP" on page 406
- "IGMP Snooping" on page 407

Static Multicast Groups

The user may define multicast groups statically via the CLI, SNMP, or Web management interfaces. For each multicast group, the user specifies a Multicast MAC Address, a VLAN identifier, and the relationship that each port of the switch has to the group. A port may relate to a multicast group in one of three ways: a port may be a permanent member, a port may be permanently forbidden from the group, or a port may be allowed to dynamically base its membership on the activity of GMRP or IGMP Snooping.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

It is important to note that the default policy of the switch is to ‘forward all multicasts.’ If static multicasts are added, then this policy should also be updated appropriately through the ‘gmrp all forward’ command.

GMRP

GMRP (GARP Multicast Registration Protocol) is defined in the IEEE 802.1D-1998 specification. Through the operation of the GMRP protocol, stations that are interested in being members of a multicast group make registration requests. The switch dynamically maintains a list of the member ports and only sends multicast frames to those ports that have members. The switch also announces to other inter-networking devices that support GMRP that the switch is a pathway to member stations. This allows member stations to “find” each other across a bridged LAN.

The management infrastructure on the CPC441x allows the user to enable and disable the operation of GMRP on a port-by-port basis or on the switch overall. In addition to the enables, the user may manage the policy used to handle Multicasts that have not been otherwise specified through Static registrations or through GMRP or IGMP. The user may statically configure a port to forward All Multicast Addresses or All Unregistered Multicast Addresses. This is done through the ‘gmrp all forward’ and ‘gmrp unregistered forward’ CLI commands.

Note: *These commands control the static ‘forward-all’ and ‘forward-unregistered’ policies even if GMRP protocol is disabled.*

The policy of whether to forward All or All Unregistered multicast addresses on a port may also be established dynamically through the operation of GMRP. A special registration called a Service Requirement registration may be signaled through GMRP to either cause All or All Unregistered multicasts to be forwarded on a port. The user may elect to ignore one or both of these service registration request types on per-port basis. This is done with the ‘gmrp all forbidden’ and ‘gmrp unregistered forbidden’ CLI commands.

GMRP has three phases of operation:

- Declaration
- Registration
- Propagation

Declarations are made by attached clients that wish to join a Multicast Group. Based on the reception of Declarations, the switch will create Registrations that define the ports that are members. Registrations may also be added Statically or via IGMP Snooping. Propagation occurs when the switch disseminates Registrations to other switches so that other GMRP participants may build registrations that include ports that are indirectly connected to the member clients.

Again, it is important to note that the default policy of the switch is to ‘forward all multicasts’. If multicast membership using GMRP is desired, then this policy should also be updated appropriately through the ‘gmrp all forward’ command.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

IGMP Snooping

The Internet Group Management Protocol (IGMP) is a protocol through which hosts and neighboring multicast agents (routers) create and maintain memberships in multicast groups on a local area network. IGMP Snooping is a mechanism used by the switch to detect which ports of the switch have devices that are interested in traffic destined to a particular Multicast Destination Address. This allows multicast packets flowing through the switch to then be forwarded only to those ports on which interested devices have been detected. This offers the potential to reduce unnecessary traffic on the network, thereby preserving bandwidth.

Two messages are used by the IGMP Protocol: Query and Report. By monitoring the IGMP Query and Report messages (“snooping”), the switch builds Layer-2 multicast domains so that it forwards the actual multicast traffic only to those ports that desire it.

The default policy of the switch is to ‘forward all multicasts’. If multicast membership using IGMP Snooping is desired, then this policy should also be updated appropriately through the ‘gmrp all forward’ command.

Multicast and IGMP Overview

A basic understanding of multicast addressing and the Internet Group Management Protocol (IGMP) is required to understand the IGMP Snooping operation.

Multicast Address Summary

IP multicast addresses are Class D IP addresses that range from 224.0.0.0 to 239.255.255.255. Multicast MAC addresses are formed by overlaying the bottom 23 bits of the Class D IP multicast address over the lower 23 bits of the base multicast MAC address value of 01-00-5E-00-00-00. Note that an IP multicast address has 28 unique bits. Consequently, each multicast MAC address can map to 32 different IP Multicast addresses.

IGMP Summary

- IGMPv1 is defined in RFC1112 and IGMPv2 is defined in RFC2236.
- IGMP is used by IP hosts to dynamically report multicast group memberships to routers.
- Like ICMP, IGMP is integrated into IP.
- IGMP uses an IP protocol number of 2.
- IGMPv1/v2 PDUs have an eight-byte payload (see RFCs 1112 and 2236 for details).
- IGMPv1 message types include:
  - host membership Query (sent by routers)
  - host membership Reports (sent by hosts)
- IGMPv2 message types, in addition to the two IGMPv1 message types, include:
  - version 2 host membership Report (sent by hosts)
  - a Leave group (sent by hosts)
- IGMPv1/v2 Queries are addressed to the **ALL-SYSTEMS** multicast group (224.0.0.1) and have an IP time-to-live (TTL) of 1. Only routers decrement the TTL in the IP header; Layer2 switches switch the packet without modifying the IP header.
- IGMPv1/v2 Reports are sent to the multicast address of the multicast group being reported (possibly 2^{23} different multicast addresses) and have an IP time-to-live of 1.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- IGMPv2 Leaves are addressed to the **ALL-ROUTERS** multicast group (224.0.0.2).
- After receiving an IGMP Query, the receiving host waits a random interval before returning its IGMP Report. If the host receives an IGMPv1/v2 Report while it is waiting for its random timer to go off, it stops the timer and does not send the associated Report for this multicast group (thus preventing duplicate IGMP Reports).
- In order to minimize IGMP overhead on hosts and networks, RFC1112 indicates that router initiated Queries are normally sent infrequently (no more than once a minute -- except at start up when several closely spaced Queries may be sent). The default General Query Interval for RFC2236 is 125 seconds; at startup, this interval defaults to ¼ of this interval until Startup Query Count Queries have been sent.
- Similar to GMRP, a host does not need be a group member in order to send datagrams to it (that is, a multicast server does not need to be a multicast group member).
- On a network without any multicast routers present, the only IGMP traffic is the occasional IGMP Report when a host joins a new host group.
- RFC2236 indicates that a multicast router that is a member of multicast groups is expected to also act as a host for those groups, and consequently, even send Reports to its own Queries.
- RFC2236 indicates that if there is more than one IGMPv2 multicast router on a network (in other words, a VLAN), only one of the routers will be a Querier; the other routers will be non-Queriers.

IGMP Snooping Functionality

The IGMP Snooping mechanism on the CPC441x limits the multicast traffic to the ports that desire to receive specific multicast groups using Layer2 techniques. The CPC441x uses IEEE 802.1Q Multicast Groups and VLANs to provide for this. Even though IGMP Snooping shares underlying switch functionality with GMRP and GVRP, it is capable of concurrent operation with, and operation without, GVRP and/or GMRP.

A Multicast Group is created automatically when IGMP Reports are received. If a Multicast Group already exists in the receiving port’s VLAN when a Report is received, then the port is added to the existing Group.

The CPC441x allows the same Multicast Group to exist in more than one VLAN. Multicast groups in different VLANs are treated separately. Multicast packets will not be forwarded across VLAN boundaries even if members of a separate Multicast Group, having the same Multicast Address, are present in the other VLAN(s).

The CPC441x employs an aging mechanism to remove Multicast Groups on a per interface and per VLAN basis from interfaces that no longer receive IGMP Reports.

IGMP Snooping monitors IGMP PDUs, and under normal conditions the CPC441x should not miss any IGMP Query or Report PDUs. Under very high IGMP PDU overload conditions, however, the CPC441x may selectively drop IGMP PDUs in favor of other traffic, such as Spanning Tree, GVRP, GMRP, and SNMP.

IGMP Snooping works for both IGMPv1 and IGMPv2.

The IGMP Snooping implementation does not discourage endnodes from sending IGMP Reports. The CPC441x does not forward Reports to non-enquiring ports. This means that two hosts on two different ports of the switch, wanting to be members of the same multicast group, will not see each other’s Report PDUs and will therefore each issue separate Report PDUs for the group. The switch needs to see Report PDUs on every port that has a member Host since the receipt of Report PDUs on a port is used to add the port to the group.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The IGMP Snooping implementation provides management support for control and monitoring (CLI Commands and MIB support for enable/disable, aging, current status per VLAN per Multicast Group). The CPC441x includes IGMP derived Multicast Group members in the RFC2674 **dot1qTpGroupTable** Multicast Group membership Table. The **dot1qTpGroupEgressPorts** object includes static, GMRP and IGMP Snooping members. The **dot1qTpGroupLearnt** object includes GMRP and IGMP Snooping members. The enable and aging control for IGMP Snooping is provided through the Performance Technologies Private MIB object Group, **cpc4400CommonIgmpSnoop**.

IGMP Snooping Operational Overview

This section provides an operational overview of the IGMP Snooping implementation.

The switch hardware device driver initializes the switch fabric to filter and forward IGMP PDUs (IP packets with a protocol number of 2) to the CPU.

On receipt of an IGMP PDU, the CPC441x performs the following:

- Each router IGMP Query for this VLAN is forwarded to each of the VLAN member ports except for the receiving port.
- All Host IGMP Reports on this VLAN for each Multicast Group are forwarded only to the IGMP querier port(s) for this VLAN. Note that the router normally expects a single Report after a Query for each multicast group, but it may receive multiple Reports due to the operation of the Snooping algorithm. Reports are only sent to the querier(s) because Reports sent to non-router ports inhibit Reports from hosts on those ports.
- Each host IGMP Leave is forwarded to each of the VLAN member ports except for the receiving port. This ensures that all attached routers will receive these messages. Note that the CPC441x does not alter the Multicast Group map for this VLAN and port based on the IGMP Leave request (there may be additional multicast hosts on this port). A port is only removed when it ages out.

For this design, the switch hardware device driver does not use the switch fabric (hardware) to forward IGMP PDUs to any of the in-band ports, but only forwards them to the CPU. The first byte of the IGMP PDU determines the PDU *type*; if any IGMP PDU type is to be forwarded to other in-band ports, it is only forwarded by the CPU using "directed" port transmits.

Table 17-1: “IGMP PDU Processing” outlines the behavior of the switch when processing IGMP PDUs.

Table 17-1: IGMP PDU Processing

First Byte of the IGMP PDU	Action
0x11 (IGMPv1/v2 *Query*)	The Port queues this PDU message to the IGMP Snooping task which, using "directed" transmits, sends this PDU to all member ports of this VLAN except for the receiving port. The Querier port number(s) for this VLAN are saved (that is, used to send IGMP Report PDUs).
0x12 (IGMPv1 *Report*)	The Port queues this PDU message to the IGMP Snooping task which, using "directed" transmits, sends this PDU to IGMP querier port(s) for this VLAN.
0x16 (IGMPv2 *Report*)	Performs the same operation as 0x12 (IGMPv1 Report), but using IGMPv2 Report PDU.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 17-1: IGMP PDU Processing

First Byte of the IGMP PDU	Action
0x17 (IGMPv2 *Leave*)	The Port queues this PDU message to the IGMP Snooping task which, using "directed" transmits, sends this PDU to all member ports of this VLAN except for the receiving port.
0xXX (anything else)	The Port drops this message (the message may be an error or an IGMPv3 type message).

The IGMP Snooping task receives PDUs from the individual Ports and Timer Event Messages from the IGMP Snooping Timer task. The IGMP Snooping task processes these PDUs/messages in the order that they are received (using a FIFO queue).

When processing an IGMP **Query** PDU message, the IGMP Snooping task:

- Adds the Query logical receive port for this VLAN ID, if it does not exist in the IGMP Snooping database.
- Clears the aging time associated with this logical Query port.
- Sends the IGMP Query PDU for this VLAN (using "directed" transmits) to each logical VLAN member port except for the logical port that received this Query.

When processing an IGMP **Report** PDU message:

- If the Multicast Group for this VLAN ID, Multicast Group and port is new (not currently in the IGMP Snooping database), the IGMP Snooping task:
  - Adds it to the IGMP Snooping database and clears the aging timer for this VLAN, Multicast Group and port.
  - Sends a message to the GARP task to add this logical port as a pseudo-static Multicast Group member for this VLAN. Note that a pseudo-static Multicast Group member is similar to a static Multicast Group member, except that the values associated with IGMP Snooping are never saved in NVM.
  - The GARP task, if necessary, creates the specified Multicast Group in the specified VLAN. Note that if this is a new Multicast Group and there is already the maximum number of Multicast Groups, GARP will not be able to create this Multicast Group and an error is returned to the IGMP Snooping task. An error is also returned if the VLAN and/or VLAN port do not already exist or if the associated **dot1qStaticMulticastForbiddenEgressPorts** bit is set for this port.
  - If the Multicast Group now exists (whether it already existed or was just created), the GARP task adds the logical port as a pseudo-static Multicast Group member.
- If the Multicast Group for this VLAN ID, Multicast Group, and logical port exists in the IGMP Snooping database, the IGMP Snooping task clears the aging time associated with this VLAN, Multicast Group and logical port.
- This IGMP Report is sent, using "directed" transmits, to each of the logical Query ports for this VLAN.

When processing an IGMP **Leave** PDU message, the IGMP Snooping task sends the IGMP Leave PDU, using "directed" transmits, to each logical VLAN member port except for the logical port that received this PDU.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

When processing an **Aging Timer Event**, the IGMP Snooping task checks each logical port member of the Group to determine if it has aged out. If so, it removes the entry from the IGMP Multicast Group. If the last port has been removed from the IGMP Multicast Group, and no GMRP or Static entries for this Multicast Group exist, then the Multicast Group is removed. When processing an **Aging Timer Event**, the IGMP Snooping task also goes through the IGMP Snooping database for each VLAN to see if any logical Query ports have aged out. Aged out logical Query ports are removed from the IGMP Snooping database.

IGMP Querier Functionality

If IGMP Snooping is enabled on the CPC441x, the user may also enable the CPC441x to be an IGMP Querier for the network. The CPC441x does not perform multicast routing, but it may be configured to send Query PDUs on a VLAN-by-VLAN basis. When enabled, the switch will arbitrate to act as the Querier as defined in RFC2236. The switch with the lowest IP Address in each VLAN is allowed to be the Querier. All other switches become ‘Non-Queriers’.

The CPC441x supports control over whether the Querier capability will be enabled for each VLAN and allows the user to establish the Query Interval and the Query Expiry times. The Query Interval specifies the frequency at which the switch will send Query PDUs to the VLAN if it is the Querier. The Expiry timer identifies how long the switch will wait before it transitions from being a Non-Querier to being a Querier when no Query PDUs are received from a lower IP Address on a VLAN.

When multiple IP Addresses are assigned to a VLAN (multi-homing), the lowest IP Address on the network interface associated with the VLAN is used as the Source Address in all Query PDUs. This IP Address is also used to compare against the Source IP Address in received Query PDUs to arbitrate for the role of Querier.

When acting as a Querier, the CPC441x will send IGMP V2 General Query PDUs to the All-Hosts Multicast Group address as defined by RFC2236.

The CLI commands provided to manage the IGMP Snoop and Query functions are described in “IGMP Snooping” on page 129.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

18

DHCP Configuration

Overview

The CPC441x supports a DHCP (Dynamic Host Configuration Protocol) server that may be used to lease IP addresses and to provide configuration information to attached clients. In addition to leasing an IP address, the DHCP server can be configured to provide the client with many other network parameters: the address of the default gateway for the client; the address of a file server; and the name of a configuration file. The file server can be the address of the CPC441x if it is to act as the file server as well as the DHCP server. The CPC441x can also act as a DHCP Relay Agent, forwarding DHCP requests to other sub-networks.

DHCP, an extension of BootP, is designed to supply clients with all of the Internet configuration parameters defined in the Host Requirements documents (RFCs 1122 and 1123) without manual intervention. Like BootP, DHCP allows the permanent allocation of configuration parameters to specific clients. The DHCP implementation provided with the CPC441x conforms to the Internet standard RFC 2131.

The CPC441x includes a DHCP client, server, and relay agent. The DHCP client can retrieve one or more sets of configuration parameters from either a DHCP or BootP server. The DHCP client also maintains any leases it has retrieved. Likewise, the DHCP server can process both BOOTP and DHCP messages. The DHCP server implementation supports all options described in RFC 2132. The DHCP relay agent provides forwarding of DHCP and BootP messages across subnet boundaries. The DHCP Client supports a subset of the RFC 2132 options (see “DHCP and BootP Client” on page 422).

The key topics in this chapter include:

- “Configuring the DHCP Server and Relay Agent” on page 414
- “DHCP and BootP Client” on page 422
- “DHCP Vendor Options” on page 422

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Configuring the DHCP Server and Relay Agent

Configuring the DHCP server and relay agent requires that the user create a pool of configuration parameter sets. When a DHCP client makes a request of the server, the server can assign a parameter set to the client (either permanently or on a leased basis). To store and maintain this pool of configuration parameter sets, the CPC441x uses a DHCP configuration file. The default filename is `dhcps.conf` located in the root directory of the CPC441x Flash file system.

Some DHCP server settings can be changed from the CLI and via SNMP. See “DHCP Client/Server Configuration” on page 91. Other DHCP parameters are established by the contents of the DHCP configuration file.

DHCP Configuration File

The DHCP configuration file is an ASCII file (**flash:/dhcps.conf**) that is used by DHCP to manage the services that are provided. This file is created (or edited) by the user. This file must be edited to modify the operation of DHCP. After changing this file, DHCP needs to be restarted. DHCP is restarted with the command:

```
dhcp server enable on
```

There is an example `dhcps.conf` file loaded on the CPC441x with all lines commented out.

The file is free format, allowing arbitrary white space characters between keywords. Lines beginning with a pound character (#) are comments, and are ignored. Long lines may be continued by ending the line with a backslash (\). Generally, no white space should precede or follow the backslash character.

The configuration file consists of two sections; a “Server Configuration / Relay Agent Section” and the “Lease Section” on page 416.

Server Configuration / Relay Agent Section

The server / relay agent configuration section of the DHCP server configuration file must precede any lease information. It has the following commands:

```
client_id_type
```

The `client_id_type` command take an integer argument indicating what value the server expects DHCP clients using PORT Client Identifier extension to use. This defaults to 0. See “Lease Section” on page 416 for more details on the PORT Client Identifier. This is a DHCP server only option.

```
client_port <port_number>
```

The `client_port` command takes an integer argument indicating to which UDP port the server should send DHCP replies. The default is 68. This option is used by both the DHCP server and relay agent.

```
interfaces <interface_name> [interface_name] ...
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The interfaces command takes a list of one or more interface on which the DHCP server should listen for DHCP requests. The CPC441x allows interface names of `sw0` and `mgmt0`. `sw0` is the name of the IP interface attached to the switched ports. `mgmt0` is the name of the IP interface attached to the Out-of-Band management Ethernet port. This option is used by both the DHCP server and relay agent.

`no_icmp_check`

By default, the switch will attempt to validate that an address is not in use on the network by sending an ICMP Echo request to the address that is about to be offered. If the address is in use, the next available address will be offered. This mode of operation is useful in cases where there are multiple DHCP servers on the network to provide redundancy, or if a switch is swapped out in place of a switch that had already provided some addresses. In cases where the leases are static, e.g., based on port or Client ID, then the validation cycle offers little benefit and slows down the DHCP process. The `no_icmp_check` command may be used to disable the verification cycle prior to making a lease offer. This is a DHCP server only option.

`port_mode`

The `port_mode` command is similar to the `client_id_type` command except that it is used in cases when a client cannot send a `client_id` or if BootP is used instead of DHCP. The `port_mode` command will cause the switch to ignore `client_id` information from the client and will assign DHCP information based on the CPC441x port number. If `port_mode` is used, the port must have only one DHCP/BootP client connected to it. This is a DHCP server only option.

See “Lease Section” on page 416 for more details.

`server_port <port_number>`

The `server_port` command takes an integer argument indicating on what UDP port the server should listen for DHCP requests. The default is 67. This option is used by both the DHCP server and relay agent.

`target_list <ip address> [ip address] …`

The `target_list` command takes an IP Address string argument indicating what DHCP server to forward incoming DHCP requests to. The DHCP server must be on a different sub-network than any of the interfaces listed. The DHCP relay agent will listen on the interfaces defined in the DHCP configuration file. This option is only used by the DHCP relay agent.

`relay_list <ip address> <netmask> [ip address] [net mask] …`

The `relay_list` command takes IP Address and Net Mask strings as arguments indicating what relay agents the DHCP server will accept DHCP requests from. The DHCP server will listen on the interfaces defined in the DHCP configuration file. This option is only used by the DHCP server.

`max_hops <max hops number>`

The `max_hops` command takes an integer number argument indicating what the max hops the DHCP server will accept incoming DHCP requests. The default is 4 and the maximum value is 16. This option is only used by the DHCP server.

`setup <begin|end>`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The setup command is used to indicate the beginning and end of the server configuration section.

Lease Section

The lease section of the DHCP server configuration file must follow the server configuration section. The lease section describes what IP addresses should be made available to DHCP clients, as well as additional parameters such as default route, address of a TFTP server, the name of a boot file to download, etc. If no leases are defined or the request does not meet requirements for a lease and the target_list has a entry all DHCP requests will be forwarded to the target server.

Each line of the lease section is a new lease, although long lines may be continued on the next line by using the backslash (\). This is still considered a single line. A lease line has the format:

```
<lease_name> <start_ip> <end_ip>
<dhcp_option:dhcp_option:dhcp_option:..>
```

The **`lease_name`** is an arbitrary string up to eight characters that uniquely identifies the lease.

While this syntax allows an entire range of addresses to be reserved, many times each DHCP client will require a unique setting (e.g., file name). In this case the `start_ip` and `end_ip` values will be the same.

The lease type is used by the server to select one of the three supported mechanisms for IP address allocation; manual, automatic, and dynamic. With manual allocation, DHCP simply conveys the related manual lease to the client. Automatic allocation assigns a permanent IP address from the corresponding automatic leases. Dynamic allocation assigns one of the dynamic leases to the client for a finite period.

Manual leases contain a specific client ID, and are issued only to that client, with an infinite duration. The example shown below specifies a MAC address, which is the identifier type used by the CPC441x DHCP client. The use of the `clid` parameter (see below) is used in the lease entry to indicate that the entry is a manual lease. Such a lease is issued only to the client with the matching type:id pair. The address range for these entries must specify a single IP address. See the sample file `dhcps.conf` in “Sample dhcps.conf Files” on page 421, “client1” uses the hardware address that the supported BootP client uses for an identifier.

Automatic leases are implied by the infinite maximum length. The IP addresses are assigned permanently to any requesting client. Setting the `maxl` parameter to 0xffffffff (infinite) is used to indicate an automatic lease. The `albp` is also used to indicate a special type of automatic lease. Setting the `albp` parameter to true in the lease entry marks the lease as suitable for BootP clients that contact this DHCP server. The IP Address will be leased for an infinite period.

Setting `maxl` to a value less than 0xffffffff indicates that this lease is dynamic. This parameter specifies the maximum lease duration granted to any requesting client. Dynamic allocation is the only method that allows reuse of addresses. The allocation type defines the priority for assigning an IP address to a DHCP client.

Manual allocations have the highest priority, and automatic allocations the lowest. Among automatic leases, configurations which are available only to specific DHCP clients are preferred.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Any parameters not specified take default values according to the Host Requirements Documents (RFC 1122 and 1123). The sample entries shown below demonstrate the possible server-issued lease types.

Many of the `dhcp_options` take values consisting of booleans, IP addresses, integers, or strings. Entries in the parameters field may be one of the types defined in Table 18-1: “DHCP Configuration Types”.

Table 18-1: DHCP Configuration Types

Type	Description
bool	Takes values of “true” or “false”, for example, ipfd=true.
str	Takes a character string as a value, for example, hstn= “clapton”. If the string includes a delimiter character, such as a colon, it should be enclosed in quotation marks.
octet	Takes an 8-bit integer in decimal, octal, or hexadecimal; for example, 070, 0xff.
short	Takes a 16-bit integer.
long	Takes a 32-bit integer.
ip	Takes a string that is interpreted as a 32-bit IP address of the form a.b.c.d. For example siad=90.11.42.1.
iplist	Takes a list of IP addresses, separated by white space, for example, rout=133.4.31.1 133.4.31.2 133.4.31.3.
ippairs	Takes a list of IP address pairs. Each IP address is separated by white space and grouped in pairs, for example, strt=133.4.27.0 133.4.31.1 133.4.36.0 133.4.31.1.
mtpt	Takes a list of 16 bit integers, separated by white space, for example, mtpt=1 2 3 4 6 8.
clid	Takes a client identifier as a value. Client identifiers are represented by the quoted string “<type>:<data>”, where <type> is an integer from 0 to 255, as defined by the IANA, and <data> is a sequence of 8-bit values in hexadecimal. The client ID is usually a MAC address, for example, clid= “1:0x08004600e5d5”. The special client identifier type 0 is by default used for DHCP clients that cannot uniquely identify themselves. The CPC441x DHCP server supports leases based on the switch port number on which a request is received. If the DHCP client sends the client identifier of 0x504F5254 (the four digit ASCII representation of “PORT”), the Ethernet port on which the request was received will be used as the client identifier. The DHCP lease pool will be searched for an entry associated with the port and the configuration information will be returned. See the sample configuration file below for an example. Options can be provided even when they are not requested (see RFC 2132 option 55 for client option requests). Any option preceded with a ‘!’ will be provided to a client; e.g.,!rout=192.168.1.250 will always give the router option regardless of the DHCP client’s request.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 18-2: “DHCP Configuration Parameters” lists the option specifiers and descriptions for every possible entry in the parameter list.

Table 18-2: DHCP Configuration Parameters

Name	Type	Description
snam	str	Optional server name.
file	str	Name of file containing the boot image.
siad	ip	Address of server that offers the boot image.
albp	bool	If true, this entry is also available to BOOTP clients. For entries using static allocation, this value becomes true by default and <maxl> becomes infinity.
maxl	long	Maximum lease duration in seconds. Only used when client requests lease time.
dfll	long	Default lease duration in seconds. If a client does not request a specific lease duration, the server uses this value. If not defined, this will be one hour.
clid	clid	This specifies a client identifier for manual leases. The CPC441x client uses a MAC address as the client identifier.
pmid	clid	This specifies a client identifier for client-specific parameters to be included in a lease. It should be present in separate entries without IP addresses.
clas	str	This specifies a class identifier for class-specific parameters to be included in a lease. It should be present in separate entries without IP addresses.
snmk	ip	Subnet mask of the IP address to be allocated. The default is a natural mask corresponding to the IP address. The server will not issue IP addresses to clients on different subnets.
tmof	long	Time offset from UTC in seconds.
rout	iplist	A list of routers on the same subnet as the client.
tmsv	iplist	A list of time servers (RFC 868).
nmsv	iplist	A list of name servers (IEN 116).
dnsv	iplist	A list of DNS servers (RFC 1035).
lgsv	iplist	A list of MIT-LCS UDP log servers.
cksv	iplist	A list of Cookie servers (RFC 865).
lpsv	iplist	A list of LPR servers (RFC 1179).
imsv	iplist	A list of Imagen Impress servers.
rlsv	iplist	A list of Resource Location servers (RFC 887).
hstn	str	Hostname of the client.
btsz	short	Size of boot image.
mdmp	str	Path name to which client dumps core.
dnsd	str	Domain name for DNS.
swsv	ip	IP address of swap server.
rpth	str	Path name of root disk of the client.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 18-2: DHCP Configuration Parameters *(Continued)*

Name	Type	Description
epth	str	Extensions Path (See RFC 1533).
ipfd	bool	If true, the client performs IP forwarding.
nlsr	bool	If true, the client can perform non-local source routing.
plcy	ippairs	Policy filter for non-local source routing. A list of pairs of (Destination IP, Subnet mask).
mdgs	short	Maximum size of IP datagram that the client should be able to reassemble.
ditl	octet	Default IP TTL.
mtat	long	Aging timeout (in seconds) to be used with Path MTU discovery (RFC 1191).
mtpt	mtpt	A table of MTU sizes to be used with Path MTU Discovery.
ifmt	short	MTU to be used on an interface.
asnl	bool	If true, the client assumes that all subnets to which the client is connected use the same MTU.
brda	ip	Broadcast address in use on the client's subnet. The default is calculated from the subnet mask and the IP address.
mskd	bool	If true, the client should perform subnet mask discovery using ICMP.
msks	bool	If true, the client should respond to subnet mask requests using ICMP.
rtrd	bool	If true, the client should solicit routers using Router Discovery defined in RFC 1256.
rtsl	ip	Destination IP address to which the client sends router solicitation requests.
strt	ippairs	A table of static routes for the client, which are pairs of (Destination, Router). It is illegal to specify default route as a destination.
trlr	bool	If true, the client should negotiate the use of trailers with ARP (RFC 893).
arpt	long	Timeout in seconds for ARP cache.
encp	bool	If false, the client uses RFC 894 encapsulation. If true, it uses RFC 1042 (IEEE 802.3) encapsulation.
dttl	octet	Default TTL of TCP.
kain	long	Interval of the client's TCP "keep-alive" in seconds.
kagb	bool	If true, the client should send TCP keep-alive messages with a octet of garbage for compatibility.
nisd	str	Domain name for NIS.
nisv	iplist	A list of NIS servers.
ntsv	iplist	A list of NTP servers.
nnsv	iplist	A list of NetBIOS name server. (RFC 1001, 1002)
ndsv	iplist	A list of NetBIOS datagram distribution servers (RFC 1001, 1002).
nbnt	octet	NetBIOS node type (RFC 1001, 1002).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 18-2: DHCP Configuration Parameters *(Continued)*

Name	Type	Description
nbsc	str	NetBIOS scope (RFC 1001, 1002).
xfsv	iplist	A list of font servers of X Window system.
xdmn	iplist	A list of display managers of X Window system.
dht1	short	This value specifies when the client should start RENEWING. The default of 500 means the client starts RENEWING after 50% of the lease duration passes.
dht1	short	This value specifies when the client should start REBINDING. The default of 875 means the client starts REBINDING after 87.5% of the lease duration passes.

BootP

The `dhcps.conf` file is also used to configure the DHCP server to support BootP clients. To support BootP clients, enter a line such as:

```
client1 90.11.42.24  90.11.42.24 \
snmk=255.255.0.0:albp=true:siad=90.11.42.26:\
brda=90.11.255.255:clid=”1:0x00c08c201020”:file=/client.conf
```

This line provides the IP address 90.11.42.24 to the BootP client with the MAC Address, 00:c0:8c:20:10:20, and will also provide the pointer to the configuration file, `client.conf`, which should be located on the server with the IP address 90.11.42.26.

Port Client ID

The Client ID is used by DHCP clients to identify themselves to the DHCP Server. This value must be unique among all clients within an administrative domain. The CPC441x DHCP configuration file maps Client IDs to IP Address bindings. Refer to the text in section 9.14 of RFC 2132 for further information on the use of Client IDs.

The CPC441x supports a Client ID that allows the lease to be based on the port where the DHCP request is received. This Client ID can be used to provide the same IP address to the client that is located on a specified port number, regardless of that client’s MAC Address. This is useful when swapping clients out of a card cage. The replacement card will get the same address as that of the card it replaces.

The Port Client ID value is a 32-bit integer set to the 4-byte ASCII sequence, “PORT” (0x504F5254).

For example, the **`dhcps.conf`** lease entry:

```
client1 90.11.42.24  90.11.42.24 clid=”0:0x07”
```

issues the IP Address 90.11.42.24 to the client located on Port 11 if that client identifies itself with the clientID type 0 and a clientID value of 0x504F5254. Only one device on each port should be configured to use this client ID value, although other DHCP clients may reside on that port using other Client ID values or no Client ID value.

If assigning IP based on port is desired, but the clients cannot provide the Port Client ID, then use the `port_mode` option described in “port_mode” on page 415. When using the `port_mode` option, however, there can only be one DHCP client on each port.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Sample dhcps.conf Files

The following sample **dhcps.conf** file illustrates the use of BootP and the use of the Lease by Port number.

```
#
setup begin
interfaces sw0
server_port 67
client_port  68
max_hops 16
# accept DHCP requests from 90.11.0.1 on subnet 90.11.0.0
relay_list 90.11.0.1 255.255.240.0
setup end

# this entry gives the IP address 90.11.42.24 to the
# card with MAC 0x00c08c102804 and it provides a
# download file name and file server address (siad)
client1 90.11.42.24 90.11.42.24 \
         snmk=255.255.0.0:albp=true:\
         siad=90.11.42.202:brda=90.11.255.255:\
         clid="1:0x00c08c102804":\
         file=config.file

# this entry uses the PORT client ID to give the
# IP address 90.11.42.25 to the card in
# slot 0x07
client7 90.11.42.25 90.11.42.25 \
         snmk=255.255.0.0:maxl=0xffffffff:\
         brda=90.11.255.255:clid="0:0x07"

# this entry issues a limitted lease from the
# pool of IP addresses in the range 90.11.42.26 to
# 90.11.42.50. The lease time is limitted to 600
# seconds regardless of the client's request. If
# the client does not specify a lease time, the
# default of 300 seconds is given.
others 90.11.42.26 90.11.42.50 \
         snmk=255.255.0.0:maxl=600:dfll=300
```

If subnetting is in effect, a critical entry in the parameters field is the subnet mask (snmk). The server does not issue addresses to clients which would change their current subnet. The address pool must specify a correct subnet mask if the default class-based mask is not valid.

The following sample `dhcps.conf` file illustrates the configuration of a Relay Agent. In this example sw0 is on vlan 1 which is connected to a DHCP Server configured to accept DHCP relay messages. Interface sw1 is on vlan 2 which is connected to a DHCP Client.

```
#
setup begin
interfaces sw0 sw1
server_port 67
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
client_port 68
max_hops 16
# Relay DHCP messages to DHCP Server 90.11.0.1.
target_list 90.11.0.1
setup end

# no leases so forward all DHCP messages on sw1 to DHCP Server in
target_list.
# if leases exist use leases first.
```

The Relay Agent will only forward DHCP messages to different subnet.

DHCP and BootP Client

The DHCP client supports the following options:

```
Client IP Address      : DHCP message “yiaddr”
Client Subnet Mask     : DHCP option 1 “snmk”
Client Default Gateway : DHCP option 3 “rout”
Boot Host              : DHCP message “said”
Bootfile               : DHCP message boot file name
```

As either a DHCP client or a BootP client, the CPC441x will configure an interface with the IP address and subnet mask provided by the DHCP server. It will also set the default gateway if the rout option is provided. Note that although the router option is a list, the client uses only the first router in the list. Upon completion of the interface and gateway configuration, the CPC441x will use the boot host and proceed to TFTP the boot file onto the flash:/ file system. When the file transfer is complete, the file will be executed.

DHCP Vendor Options

To support the RFC 2132 DHCP Vendor Options in the DHCP Server feature, the following functionality has been added.

The `vendor_opts` line in the setup section of the DHCP server configuration file configures the vendor name and vendor data. Only one vendor option name and data may be entered on a vendor_opts line. Multiple vendor_opts lines may be present in the DHCP server configuration file. The vendor name and vendor data may be entered as either Hex or ASCII character data. Each field must not exceed 255 bytes. If entered as ASCII character data and spaces are present, the value MUST be enclosed in double quotes. The double quotes are optional if no spaces are present, and for Hex data. Hex data MUST be preceded with 0x. As this adds compatibility for other vendor's unique features, there is no checking for the validity of either the vendor name or vendor data.

Example

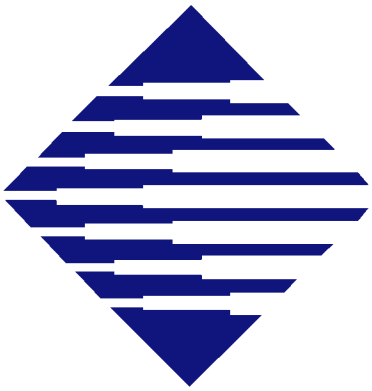
```
setup begin
interfaces sw0
vendor_opts "pti vclass id 1" "0x0104ffffff00" \
                      "0x1234" "0x03040a010101"
setup end
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

In this example the first class id string is `pti vclass id 1`, when provided by a client would return the hex string option which breaks down to dhcp option 1 (subnet mask) size 4 value 255.255.255.0. In the second entry the vendor class id is given as a hex string and the information is option 1 (router) size 4 value 10.1.1.1.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Chapter

19

File System

Overview

This chapter describes the Flash file system that provides permanent storage for the CPC441x. The key topics in this chapter include:

- “Remote File Systems” on page 426
- “Special Files” on page 427
- “Installing the CPC441x Application Software Image” on page 430
- “Upgrading the CPC441x Boot Files” on page 431
- “Board Application Software Recovery Procedure” on page 432
- “Configuring CPC441x Software” on page 440

General

The CPC441x uses an 8 megabyte (MB) Flash file system device to provide permanent storage. This storage holds such things as the system application program, the saved configuration, user scripts, etc. Of the 8 MB, 6 MB is reserved for the board operating system, leaving 2 MB available to the user. While nothing restricts the user from consuming more than 2 MB, future releases of board software may require the entire 6MB that is reserved for the board operating system.

The contents of the Flash file system are maintained across re-boots, and while the system is turned off. The drive name of the Flash file system device is `flash:`.

The CPC441x also has a 1 MB RAM-based file system for temporary files. This device is provided entirely for the user, and may be used for such things as temporary scratch space during the boot process, or as a faster alternative to the Flash device. The contents of the RAM-based file system are lost during a reboot. The drive name of this device is `ramdisk:`.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

File and directory names are restricted to 40 characters, and special characters such as asterisk (*), slash (/), and backslash (\) should not be used. File names are not case sensitive; a file named **aBcD** is the same as one named **AbCd**.

In order to efficiently maintain the file system, a certain amount of free space is required. It is recommended that at least 10% of the file system space be left unused. Supported configurations will always provide the entire 2 MB available to the user.

Note: *The root of the file system(s) can hold up to 128 files and/or directories.*

File System Commands

Commands to manage files on the file systems are described in “File System Management” on page 100.

Remote File Systems

The CPC441x provides the capability to allow a remote device to appear as if it is a local file system. The `mount` command is used to attach the remote device to the system. Once attached, the remote device can be treated as a regular file system, using commands such as list and copy. The only requirement of the remote device is that it supports remote FTP access, and that the user have a valid user ID and password on that system. The general convention when attaching a remote system is to use the name of the system followed by a colon as the name of the file system (or mount point).

For example, if the system `host1` has the IP address 10.0.0.1, the following command would be used:

```
mount host1: 10.0.0.1
```

The switch then prompts for the host user-id and password. Alternatively, the host user-id and password could also be specified on the command line. The CPC441x only retains the user-id and password of the last device mounted. If multiple remote devices require a distinct user ID or password, only the most recently mounted device will be accessible, and the error “Login incorrect” will be displayed when accessing the earlier device.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Special Files

The following files have special significance, and extra care should be taken when dealing with them.

cpc4411.Z / cpc4416.Z

This file (hereafter "`cpc441x.Z`") contains the CPC441x application program (operating system). It is required in order for the board to operate. See "Update System Files" on page 238 and "Installing the CPC441x Application Software Image" on page 430.

durable

This file contains the switch settings saved to file using the `save` command. These settings are restored using this file during the boot process. If the file does not exist, the factory default settings will be used. See "Save the Switch Configuration" on page 104 for more details.

persist

The settings in this file will not change with a restore of factory defaults. The product name is the only object in this file.

Note: *The format of the **durable** and **persist** files is specific to each software release. This means that a **durable** or **persist** file created with one version of the software is not necessarily compatible with another version of the software. When performing a software version change, it is recommended that the user capture the configuration parameters into a script file by using the 'running' command (the CLI syntax of each software version is intended to be backward-compatible with previous versions). See "Capturing a Configuration to a CLI Script" on page 443.*

dhcps.conf

This user-maintained file contains the data necessary to configure the DHCP server. If this file does not exist, and the DHCP server is enabled, the system will issue a warning. See Chapter 18, "DHCP Configuration," on page 413 for more details.

log.msg

When "logging to a file" is enabled, `log.msg` is the default file where log messages are placed. If the file is erased, logging to a file will be suspended until the system is restarted, at which point a new file will be created. If the file exists during boot, log messages will be appended to the end of the file. See "Log Management" on page 172 for more details.

Note: *It is best to archive and then remove the `log.msg` file periodically to avoid consuming large amounts of file system space.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

boot.lua

boot.lua is a user defined Lua script file. It is automatically executed during the CPC441x boot process. It is executed after the **durable** file has been loaded and its settings have been instantiated, but prior to the initialization of the CPC441x TCP/IP stack. This provides a mechanism for the user to override NVM settings that affect the initialization of the TCP/IP stack, such as DHCP Client Enable, DHCP Client Identifier, IP Network Interface Addresses, etc.

The user simply creates a file named **boot.lua** and places it on the CPC441x in the root directory and the CPC441x will execute it each time the card is booted. The existence of this file is not required.

Typically, **boot.lua** would contain Lua code that would modify the CPC441x IP settings using the IDB access library. The following is an example **boot.lua** that sets the DHCP Client ID based on the slot number the CPC441x is located in and enables DHCP via sw0. See Chapter 21, “Lua Programming Language,” on page 449 for more information.

```
-- Get slot number

slot = idbU32Get("cpc4400:cpc4400CommonMiscSlotID", 0)

-- Get shelf number

shelf = idbU32Get("cpc4400:cpc4400CommonMiscShelfID", 0)

-- Set Client ID to include shelf and slot number

idbOctetStringSet("cpc4400:cpc4400CommonMiscDHCPClientID", 0, "\07SLOTnSHELF" ..
strchar(shelf, slot))

-- Set VLAN ID for DHCP

cli(“dhcp client vid 1”)

-- Enable Interface for DHCP

cli(“dhcp client enable sw0 on”)
```

rc.lua

rc.lua is a user-defined Lua script file. It is automatically executed following the CPC441x boot process. This provides a mechanism to allow the user to establish customized run-time settings. See Chapter 21, “Lua Programming Language,” on page 449 for more information.

Message of the Day

A message of the day is presented when a user logs into the switch via FTP, Telnet, SSH, and console access. The message consists of two special files: **flash:/prelogin_banner** and **flash:/postlogin_banner**.

- If the file **flash:/prelogin_banner** is present on the switch, it will be displayed when a user connects to the switch via console port, Telnet, FTP, SFTP, or SSH before logging in.
- If the file **flash:/postlogin_banner** is present on the switch, it will be displayed when a user connects to the switch via console port, Telnet, FTP, or SSH after logging in. This feature is **NOT** supported with SFTP.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Note: *The prelogin banner message is sent in SSH and SFTP as per Section 5.4 of RFC 4252. As this is an optional feature of the SSH and SFTP clients, not all clients may display this message. This has been successfully tested with SSH clients PuTTY version 0.60 running on Windows XP, OpenSSH_4.2p1 with OpenSSL 0.9.8a 11 Oct 2005 running on SuSE Linux, and OpenSSH_4.7p1 with OpenSSL 0.9.8g 19 Oct 2007 running on Ubuntu Linux.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Installing the CPC441x Application Software Image

The following procedures are used to upgrade or change the board-level operating software. Generally, these procedures are not required, and software replacement should be undertaken only upon receiving instruction to do so from Performance Technologies Technical Support.

The software image on the CPC441x switch may be installed using a TFTP server. A TFTP server application must be installed on a TCP/IP-ready workstation. As of this writing, TFTP server software for Windows 98 and Windows NT can be found at no charge at the following URL:

http://www.solarwinds.net

Check the IP address of the TFTP server and the CPC441x targeted for the TFTP software upgrade to be sure the addresses are within the same range (the same subnet). Ping the TFTP server from the CPC441x to verify that a network connection exists between them.

1. Acquire the new software from Performance Technologies. This will typically be in the form of a .zip file.
2. Unzip the software on your TFTP server.
3. Read the Release Notes for any special instructions, bug fixes, new features, etc.
4. If you wish to retain the existing configuration of the switch after the upgrade, then follow the recommendations described in “Capturing a Configuration to a CLI Script” on page 443.
5. Establish network connectivity between the CPC441x and the TFTP Server.
6. Transfer the provided installation script to the CPC441x (install.lua).
7. Execute the install script and answer questions. This will transfer the new files to the board, install them, and reboot the switch.

Following is an example:

```
# ip config mgmt0 192.168.1.2 255.255.255.0
# tftp get 192.168.1.1 /release5r1/install.lua install.lua
# install
```

In this example, the switch is provided with an IP Address, and the install script (**install.lua**) is transferred from the server located at 192.168.1.1. The upgrade files had previously been unzipped on the server in the directory **/release5r1**. Finally, the script is executed by name. The script will prompt you for the IP address of the server and the path to the upgrade files.

The current Application file will be saved under a new name which will be displayed during the installation. If your existing software version supports it, the current configuration will be captured using the `running` command. In some cases, you may have customized a provided file for your own use, such as **rc.lua** or **boot.lua**. If the file included in the installation package differs from the one on the switch, you will be prompted to accept the new file or to keep your current file.

The board needs to be rebooted before the new image will take effect.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Upgrading the CPC441x Boot Files

The boot function of the CPC441x is implemented in three stages: low level initialization, execution of the boot script, and loading of the application. Each of these stages is supported by a separately maintained object. Each object can be upgraded individually. These objects are upgraded by transferring a file containing the object image(s) to the CPC441x file system, and then invoking the `switch install` command(s) to store the image(s) in the proper non-volatile memory area. The object image files that support the boot process on the CPC441x are: **rom.sf**, **script.4th**, and **bootloader.bin**. It is unlikely that the boot files will ever need updating. Should the need arise, however, use the following procedure.



Caution:
Always use the CPC441x boot files provided by Performance Technologies. Both the TFTP and the `switch install` commands will install any file. If the wrong (or a corrupt) file is installed, the CPC441x will not boot and the board must be returned to Performance Technologies for repair.



Caution:
Before installing any boot files, issue a "port link all down" to minimize traffic on the switch. Boot files should be installed with a high priority to reduce the risk of an install error. In the event of an error, the board must be returned to Performance Technologies for repair.

The object image files that support the boot process on the CPC441x are: **rom.sf**, **script.4th**, and **bootloader.bin**.

1. Use a TFTP server to download the new object image file into the Flash memory using the following CLI command:

```
tftp get <ip_host> <source_file> <destination_file>
```

For example, if the TFTP server's IP address is 192.168.1.1 and the boot files are located in the ***/my_account*** directory, then the TFTP commands are:

```
tftp get 192.168.1.1 /my_account/rom.sf rom.sf
tftp get 192.168.1.1 /my_account/scripts.4th scripts.4th
tftp get 192.168.1.1 /my_account/bootloader.bin bootloader.bin
```

2. Use the `switch install` commands to program the new boot files into the CPC441x using the following commands.

```
switch install rom rom.sf
switch install bootscript script.4th
switch install loader bootloader.bin
```

Each invocation of this command will indicate the file size and CRC-32 for the specified file. Please insure that this is the same as the information provided in the **fileinfo.txt** file provided with the upgrade.

Reboot the switch to allow the new Boot software to take effect.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Board Application Software Recovery Procedure

Use the following procedure to reinstall the application software stored in Flash memory.

By default, the CPC441x uses the `cpc441x.Z` application image when powering up. If this image becomes corrupted during the software upgrade process, you have several options:

- If you have not yet rebooted the switch, repeat the software upgrade process.
- If there is another application software image in Flash, you may use the procedures described below to select the other image.
- If the switch does not have a valid image in Flash, then the board can still boot an image located on a TFTP or FTP server.

The VxWorks Boot Shell

The CPC441x uses VxWorks for its underlying operating system. The VxWorks Boot shell provides a mechanism to select the source of the image to be booted. This is done through the definition and selection of a 'boot string.' A boot string defines the source file system or LAN interface device where the image is located, the name of the image, the Client and Server IP Addresses to use if booting from a LAN, user name and password information, and selection of transfer protocol to use. The management port is used to boot from the LAN.

Three boot strings are supported. These allow the user to have a boot string definition to boot from Flash and two others to boot from the network or to boot alternate images in Flash. When a switch is shipped, boot string number 0 typically defines the Performance Technologies manufacturing boot string used to initialize the board at the factory, boot string number 1 typically selects the Flash Image (selected by default), and boot string number 2 is undefined. In the following recovery scenarios, the user is directed to select boot string number 2, define the parameters to boot from the network, boot from the network and restore the Flash image, and finally select boot string number 1 to boot from Flash again.

The VxWorks boot shell is entered by resetting the card with a console attached and holding down the space bar during the boot. The boot process will be interrupted and the shell will be invoked. The VxWorks Boot Shell prompt looks like:

```
[VxWorks Boot]:
```

The following commands are available at this shell:

```
E - Erase Flash (be careful with this one)
R - Reset the switch
b - Select a boot string
c - Configure the selected boot string
p - Print the boot string
```

The following commands are available if Flash was selected as the boot device when the system was last booted:

```
ls - List the contents of the Flash Filesystem
rm - Remove a file
cp - Copy a file
```

A boot string has the following parameters:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
Boot string          : <0, 1, or 2>
Boot device          : <selects Flash or Management Port>
Unit number          : 0
Processor number     : 0
Host name            : <your server name>
File name            : <name of the image>
Inet on ethernet (e) : <IP address>:<netmask>
Host inet (h)        : <server IP address>
Gateway inet (g)     : <gateway IP address>
User (u)             : <user login>
ftp password (pw)    : <User password>
Flags (f)            : <selects transfer protocol>
target name (tn)     : <gives a name to your switch>
```

The boot string parameters are described here in more detail:

Boot Device enter ‘tffs=0,0’ to boot from Flash, or ‘mgmt0’ to boot from the Management Ethernet port.

Host name You may optionally provide the name of your LAN server.

File name Enter the complete path and filename of the application image file. The default image name is ‘`/tffs/cpc4411.Z`’ or ‘`tffs/cpc4416.Z`’. The file must be a VxWorks compressed image. The name must end with ‘.Z’ (capital Z) defining the file type to the boot loader. If booting from the LAN, one of three transfer protocols is used: rsh, ftp, or tftp. The choice is dictated by the value of the Flags field, and the presence or absence of an ftp password; both are described below. If rsh is used, then the user must have an account with proper permissions on the server, and the file name may be given as a relative path from the user’s home directory. The rsh protocol will be used to execute the unix `cat` command to retrieve the boot image.

Inet on Ethernet The IP Address used by the switch to load a boot image from the LAN is determined by this boot parameter. This parameter is provided in the format IPAddress**:**SubnetMask, where the IPAddress portion is given in dotted decimal notation and the SubnetMask portion is given in Hex format (ffffff00 represents 255.255.255.0). For example, the IP Address 192.168.1.2 with a Subnet Mask of 255.255.255.0 is represented as 192.168.1.2**:**ffffff00.

Host Inet This parameter defines the IP Address of the Server. If it is not on the same subnet as the switch, then the user must provide a gateway address as described below. This parameter is provided in dotted decimal format and does not include the subnet mask. For example, 192.168.1.1.

Gateway Inet This parameter defines the IP Address of the gateway to use if the Server is on a different subnet than the switch. The gateway address MUST be on the same subnet as the switch. This parameter is provided in dotted decimal format and does not include the subnet mask. For example, 192.168.1.100.

User This parameter defines the User ID to use when loading from the LAN using rsh or ftp.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

FTP Password This parameter must be provided if using ftp as the transfer protocol. It should be left blank if using rsh.

Flags This parameter selects various options. The only options that may need to be selected by the user are whether TFTP is used for the LAN transfer protocol and whether to delay the boot process. This parameter is a bit-mask. The only two bits described here are bits 3 (0x8) and 7 (0x80). Bit 3 selects boot with no delay. If bit 3 is off, then an eight second delay is introduced into the boot process to allow the user more time to interrupt the boot. Bit 3 is normally left on for faster boot. Bit 7 selects TFTP as the transfer protocol. If bit 7 is on, and the boot device is mgmt0, then the transfer will be TFTP. If bit 7 is off, and the boot device is mgmt0, then the transfer will be either rsh or ftp. If the ftp password is defined, then ftp will be used; otherwise rsh will be used.

Target Name This parameter gives a hostname to your switch. It can be used in conjunction with the use of 'rsh' to download a new image to the switch. If TFTP or FTP are used to boot from the network, then this parameter is not required.

Use the b command to select one of the three boot strings. For example:

```
[VxWorks Boot]: b 2
```

Use the c command to configure the boot string. The boot string parameters will be displayed one line at a time. Type the new value or <CR> to leave the value unchanged. Enter a single period ('.') on a line to erase a parameter. The minus symbol ('-') can be used to go up one line.

Use the p command to display the current boot string. Use this command after making changes to verify that all the settings are correct.

In order to reboot the switch after configuring the boot string, use the R command. You may be familiar with the VxWorks @ command to continue with the boot process, but this command does not work if Flash was selected as the boot device when the system was last booted.

The E command is provided to allow the Flash to be completely erased. This command should be used only if you know that you are able to boot from the network. If you erase Flash and boot from the network, the application code will automatically reformat the Flash file system as it boots. After you boot, you can use the software installation process to completely recreate a factory configuration.

Note: *The E command will also erase any stored configurations and script files.*

Booting the CPC441x with an Alternate Image Stored in Flash Memory

If the `cpc441x.Z` application image in Flash memory was deleted or damaged but an alternate image is located in Flash, then use these procedures to select the alternate image.

If there was an attempt to boot the board with a corrupt `cpc441x.Z` image, the following error message is displayed:

```
Cannot open "/tffs/cpc441x.Z"
Error loading file:  error 0x3800003.
```

1. Reboot the CPC441x again and stop the boot sequence by holding the space bar during the boot process.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The switch stops at the VxWorks boot prompt displaying:

```
[VxWorks Boot]:
```

2. Press c to enter the boot editor and then continue to press Enter until you get to the following line:

```
file name : /tffs0/cpc441x.Z
```

3. Type the correct file name, for example:

```
/tffs0/cpc441x_old.Z
```

For example, if the application image stored in Flash memory is named `cpc441x_old.Z`, then change the file name to `cpc441x_old.Z`.

4. Continue to press Enter until you are out of the boot editor. Then type R to continue the boot process.

The board boots with the specified File name (`cpc441x_old.Z`).

The software upgrade process can resume. See “Installing the CPC441x Application Software Image” on page 430. After the application software has been successfully downloaded into the Flash memory, reboot the switch and change the `File name` in the boot sequence back to `cpc441x.Z` using the same procedure.

Booting the CPC441x from a TFTP server

Use the following procedure to boot the board from a TFTP server.

If there was an attempt to boot the board with a corrupt `cpc441x.Z` image and there is a boot failure, the following error message is displayed:

```
Cannot open “/tffs/cpc441x.Z”
Error loading file:  error 0x3800003.
```

1. Reboot the CPC441x again and stop the boot sequence by holding the space bar during the boot process.

The switch stops at the VxWorks boot prompt displaying:

```
[VxWorks Boot]:
```

2. Type p to see the boot sequence and note the currently selected boot string.

```
[VxWorks Boot]   : p
boot string      : 1
boot device      : tffs=0,0
unit number      : 0
processor number : 0
host name        : cpc441x
file name        : /tffs0/cpc441x.Z
flags (f)        : 0x8
target name (tn) : cpc441x
```

3. Use the b command to select an alternate boot string. For example ‘b 2’
4. Type c and continue pressing Enter until you get to the boot fields you want to change and type the appropriate information as follows:
   - Change **`boot device`** from `tffs=0,0` to `mgmt` (the out-of-band management port).
   - Change **`file name`** to provide the path and the name of the application image stored on your server.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- Change **flags** to 0x88 to enable a TFTP boot.

5. Continue to press Enter until you exit the boot editor. Type **p** to verify that the new boot sequence is correct. The boot sequence should appear as follows:

```
Boot string          : 2
Boot device          : mgmt
Unit number          : 0
Processor number     : 0
Host name            : <your server name>
File name            : /path/cpc441x.Z
Inet on ethernet (e) : <IP address[1]>:<netmask[2]>
Host inet (h)        : <server IP address>
Gateway inet (g)     : <gateway IP address>
User (u)             : <user login>
Flags (f)            : 0x88
```

6. Ensure the management port is connected to the network and is on the same subnet as your TFTP server. If the TFTP server is not on the same subnet, then the `gateway inet (g)` field needs to specify an IP address of the gateway, which connects the TFTP server subnet.
7. Type `R` to reboot. The switch will now boot an image from the TFTP server. Note that this does not transfer the image to Flash. It simply loads the image into RAM and executes it. You still need to install the image to Flash before you are ready to boot from Flash.
8. Perform the software installation procedure as described in “Installing the CPC441x Application Software Image” on page 430.
9. Reboot the switch and stop at the boot prompt by holding the space bar during the boot process. Use the `b` command to select the original boot string noted in Step 2. This will change the boot sequence to let the switch boot from the updated image stored in the Flash memory.
10. Type `R` to reboot. The switch will now boot using the new application image stored in Flash.

Booting the CPC441x from an FTP server

Use the following procedure to boot the board from an FTP server.

If there was an attempt to boot the board with a corrupt `cpc441x.Z` image and there is a boot failure, the following error message is displayed:

```
Cannot open “/tffs/cpc441x.Z”
Error loading file:  error 0x3800003.
```

1. Reboot the CPC441x again and stop the boot sequence by holding the space bar during the boot process.

   The switch stops at the VxWorks boot prompt displaying:

   ```
   [VxWorks Boot]:
   ```

[1] This is the IP addresses assigned to the CPC441x in dotted-decimal format (e.g., 192.168.1.2).

[2] This is the IP addresses netmask associated with the CPC441x IP Address. It is in Hex format (e.g., ffffff00) ffffff00=255.255.255.0.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

2. Type `p` to see the boot sequence and note the currently selected boot string.

```
[VxWorks Boot]   : p
boot string      : 1
boot device      : tffs=0,0
unit number      : 0
processor number : 0
host name        : cpc441x
file name        : /tffs0/cpc441x.Z
flags (f)        : 0x8
target name (tn) : cpc441x
```

3. Use the `b` command to select an alternate boot string. For example ‘b 2’
4. Type `c` and continue pressing Enter until you get to the boot fields you want to change and type the appropriate information as follows.
   - Change **`boot device`** from `tffs=0,0` to `mgmt` (the out-of-band management port).
   - Change **`file name`** to provide the path and the name of the application image stored on your server.
   - Change `User` and ftp `password` fields to appropriate values for your server.
   - Set the `Flags` field to 0x8.
5. Continue to press Enter until you exit the boot editor. Type **p** to verify that the new boot sequence is correct. The boot sequence should appear as follows:

```
Boot string         : 0
Boot device         : mgmt
Unit number         : 0
Processor number    : 0
Host name           : <your server name>
File name           : cpc441x.Z
Inet on ethernet (e): <IP address[3]>:<netmask[4]2>
Host inet (h)       : <IP address of the FTP Server>
Gateway inet (g)    : <gateway IP address>
User (u)            : <user login>
ftp password (pw)   : <User password>
Flags (f)           : 0x8
```

[3] This is the IP addresses assigned to the CPC441x in dotted-decimal format (e.g., 192.168.1.2).

[4] This is the IP addresses netmask associated with the CPC441x IP Address. It is in Hex format (e.g., ffffff00) ffffff00=255.255.255.0.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

6. Ensure the management port is connected to the network and is on the same subnet as your FTP server. If the FTP server is not on the same subnet, then the `gateway inet (g)` field needs to specify an IP address of the gateway, which connects the FTP server subnet.
7. Type `R` to reboot. The switch will now boot an image from the FTP server. Note that this does not transfer the image to Flash. It simply loads the image into RAM and executes it. You still need to install the image to Flash before you are ready to boot from Flash.
8. Perform the software installation procedure as described in “Installing the CPC441x Application Software Image” on page 430.
9. Reboot the switch and stop at the boot prompt by holding the space bar during the boot process. Use the `b` command to select the original boot string noted in Step 2. This will change the boot sequence to let the switch boot from the updated image stored in the Flash memory.
10. Type `R` to reboot. The switch will now boot using the new application image stored in Flash.

Booting the CPC441x from a Unix Server Using ‘rsh’

Use the following procedure to boot the board from a Unix server. This method uses the Remote Shell (rsh) facility supported on most Unix servers. The user must have access privileges on the server. The UNIX system restricts network access through remote login, remote command execution, and remote file access. This is done for a single user with the .rhosts file in that user's home directory, or globally with the **/etc/hosts.equiv** file.

The .rhosts file contains a list of system names that have access to your login. Thus, to allow a switch named `cpc4400` to log in with your user name and access files with your permissions, create a .rhosts file in your home directory containing the line:

```
cpc4400
```

The **/etc/hosts.equiv** file provides a less selective mechanism. Systems listed in this file are allowed login access to any user defined on the local system (except the super-user **root**). Thus, adding the switch name to **/etc/hosts.equiv** allows the switch to log in with any user name on the system.

Follow these steps to boot from a Unix Server using the ‘rsh’ mechanism:

1. Reboot the CPC441x again and stop the boot sequence by holding the space bar during the boot process.

   The switch stops at the VxWorks boot prompt displaying:

   ```
   [VxWorks Boot]:
   ```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

2. Type `p` to see the boot sequence and note the currently selected boot string.

```
[VxWorks Boot]   : p
boot string      : 1
boot device      : tffs=0,0
unit number      : 0
processor number : 0
host name        : cpc441x
file name        : /tffs0/cpc441x.Z
flags (f)        : 0x8
target name (tn) : cpc441x
```

3. Use the `b` command to select an alternate boot string. For example, ‘b 2’
4. Type `c` and continue pressing Enter until you get to the boot fields you want to change and type the appropriate information as follows.
   - Change **`boot device`** from `tffs=0,0` to `mgmt` (the out-of-band management port).
   - Change **`file name`** to provide the path and the name of the application image stored on your server.
   - Change the `User` parameter to your Unix User ID.
   - Ensure that the ftp `password` parameter is blank (type ‘.’ to erase an existing value).
   - Set the `flags` field to 0x8.
   - Set the `target name` field to the name of the switch (matching the value used in your **.rhosts** file).
5. Continue to press Enter until you exit the boot editor. Type **p** to verify that the new boot sequence is correct. The boot sequence should appear as follows:

```
Boot string          : 0
Boot device          : mgmt
Unit number          : 0
Processor number     : 0
Host name            : <your server name>
File name            : cpc441x.Z
Inet on ethernet (e) : <IP address[5]>:<netmask[6]>
Host inet (h)        : <IP address of the FTP Server>
Gateway inet (g)     : <gateway IP address>
User (u)             : <user login>
ftp password (pw)    :
Flags (f)            : 0x8
target name (tn)     : cpc441x
```

[5] This is the IP addresses assigned to the CPC441x in dotted-decimal format (e.g., 192.168.1.2).

[6] This is the IP addresses netmask associated with the CPC441x IP Address. It is in Hex format (e.g., ffffff00) ffffff00=255.255.255.0.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

6. Ensure the management port is connected to the network and is on the same subnet as your Unix server. If the server is not on the same subnet, then the `gateway inet (g)` field needs to specify an IP address of the gateway, which connects the server subnet.
7. Type `R` to reboot. The switch will now boot an image from the server. Note that this does not transfer the image to Flash. It simply loads the image into RAM and executes it. You still need to install the image to Flash before you are ready to boot from Flash.
8. Perform the software installation procedure as described in “Installing the CPC441x Application Software Image” on page 430.
9. Reboot the switch and stop at the boot prompt by holding the space bar during the boot process. Use the `b` command to select the original boot string noted in Step 2. This will change the boot sequence to let the switch boot from the updated image stored in the Flash memory.
10. Type `R` to reboot. The switch will now boot using the new application image stored in Flash.

Booting the CPC441x from Another CPC441x

Another CPC441x that has a valid application image on it may be used as the TFTP or FTP Server to boot a board that has a corrupted image. Simply follow the steps outlined in “Booting the CPC441x from a TFTP server” on page 435, or “Booting the CPC441x from an FTP server” on page 436, using the CPC441x as the Server. Note that if you use FTP, then you must configure the FTP Daemon userid and password on the server switch as follows:

```
# ftpd userid user
# ftpd password password
```

Configuring CPC441x Software

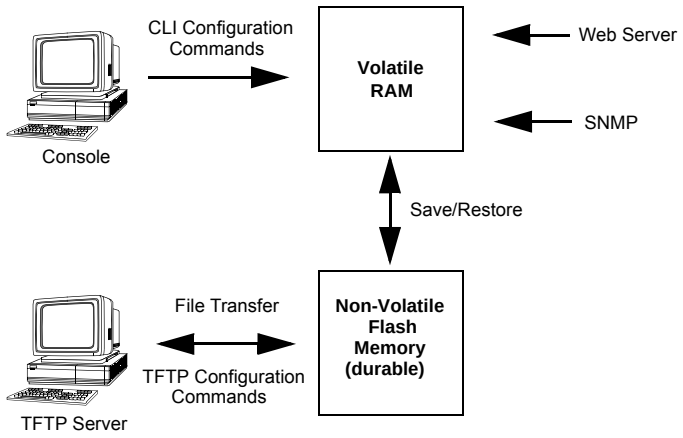
The CPC441x uses information from the configuration files when it starts up. The configuration files contain all of the “durable” MIB parameters shown in “Durable MIB Parameters” on page 263.

These configuration files are named **persist** and **durable**; they exist (with factory defaults) before any custom configuration is done.

Switch configuration information can be generated by several means. Configuration commands can come from a terminal (CLI commands), SNMP, or via the Web server. See Figure 19-1: “Memory and Configuration Files” on page 441.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 19-1: Memory and Configuration Files



When configuring the CPC441x (using CLI commands, SNMP, or the Web), the current running configuration that operates out of RAM is changed. To store the configuration into non-volatile Flash memory, the following command must be used:

```
save
```

The `save` command stores the running configuration information (in RAM) into the **durable** and **persist** files in the Flash memory. Several different configuration files can be stored inside the Flash with different names. For example, current Flash settings can be saved under different filenames as a backup if it becomes necessary to restore them later. This allows experimentation with current settings while maintaining the ability to restore original settings if something goes wrong.

Note: *The format of the **durable** and **persist** files is specific to each software release. The **durable** and **persist** files contain only those non-volatile settings that are known by the software used to create them. Every attempt is made to ensure compatibility between software revisions. If an incompatibility exists between revisions, it will be identified in the Release Notes document. If a parameter that existed in a prior release is removed in a later release, the new software will display a warning message during the boot process. Any newly added parameters will be automatically set to default values. All other parameters will be set from the old **durable** file. Once the new software is booted, executing the `save` command will create a new **durable** file compatible with the new revision of code. This will eliminate any warnings at the next reboot.*

The **durable** or **persist** files can be transported using any of the provided file transfer methods (TFTP, FTP, copy, etc.). Copy the **durable** configuration file to a different filename before making any changes to the current configuration and storing them into the Flash. Use the following command:

```
copy <filename1> <filename2>
```

Copy **durable** to a different filename (`saved_durable`) before applying any changes to the switch. If you decide to restore the previous configuration (the one you saved as `saved_durable`), copy the saved configuration file into the **durable** file and execute the `switch reset` command to reset the CPC441x with the desired configuration.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The command syntax is:

```
copy saved_durable durable
switch reset
```

There is a special `switch install` command, which does the same thing as the `copy` command. Use this command to copy the desired configuration file to the **durable** file. The syntax is as follows:

```
switch install config saved_durable
switch reset
```

Both the `copy` and the `switch install config` commands copy the specified configuration file to the **durable** file. The only difference is in the syntax.

In this example, a configuration file is copied from a TFTP server to the CPC441x:

```
tftp get <host_ip> <source_file> <destination_file>
```

where

`host_ip`	is an IP address of the TFTP server
`source_file`	is an ASCII string specifying the path to and name of the source file.
`destination_file`	is an ASCII string specifying the path to and name of the destination file

You can store the configuration file on the TFTP server using the command:

```
tftp put <host_ip> <source_file> <destination_file>
```

Whenever you download the configuration file from the TFTP server into the switch always select a *destination_file* name different from the **durable** and then use the `copy` or the `switch install` command to copy the desired configuration to the **durable**. This may avoid destroying the original configuration in case of a transfer error. The *destination_file* will be destroyed if you specify a wrong TFTP server IP address, make a mistake by typing a wrong path or filename, or if your TFTP server is not configured properly. The following is an example of commands to load the configuration file into the switch:

```
tftp get 192.168.1.1 /my_path/durable new_durable
copy new_durable durable
switch reset
```

The following is an example of using the `switch install` command instead of a `copy` command:

```
tftp get 192.168.1.1 /my_path/durable new_durable
switch install config new_durable
switch reset
```

Remember that downloading a configuration file into the Flash and copying it to the **durable** file does not affect the running configuration. To reprogram the switch with the configuration information stored in the **durable** file, you need to reboot the switch.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Restoring the CPC441x Factory Default Settings

Use the `switch defaults` command to reboot the board and restore the factory default settings that are stored in permanent memory. The board will initialize with the factory defaults. See “Reset the Switch to Factory Default Values” on page 237 for command details.

Capturing a Configuration to a CLI Script

Another method to manage switch configuration is by using the `running` command (see “Capture Current Configuration into a CLI Script File” on page 105). This command generates an ASCII file composed of CLI commands that generate the current “running” configuration. The file generated - flash:/running.cli - may be transferred off-board, edited to make changes, or loaded onto other boards and executed. To execute the file, type:

```
running.cli
```

This command is recommended when performing software revision changes. The CLI syntax is intended to remain backward-compatible with earlier software versions. This allows the configuration of the board to be captured into a CLI script prior to performing the upgrade, and then re-instantiated after the upgrade is performed.

The `running` command creates a CLI script file that captures all of the parameters stored in the **durable** file. All parameters settings are captured into a file called ‘running.cli.

Here are the steps required to restore the configuration of a switch that has routing protocols enabled:

1. Create the **running.cli** and **route_config.cli** scripts using the `running` command.
2. Execute the **running.cli** script.
3. Execute the `save` command to store the settings.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

20

Diagnostic Tools

Overview

The CPC441x provides a set of tools that allow the user to diagnose network problems. These tools are broken into two groups: mirror tools and connectivity tools. The mirror tools allow the user to reflect packets from one port to another port. An analyzer can be placed on a fixed port and the user can dynamically have any other port's traffic reflected to the analyzer port. The connectivity tools include ping and traceroute, which are useful in verifying or diagnosing connectivity problems on an IP network.

The key topics in this chapter include:

- "Port Mirrors" on page 445
- "Ping" on page 446
- "Traceroute" on page 446
- "Embedded Diagnostics" on page 446
- "Fault State" on page 448

Port Mirrors

The Port Mirror tools can be used to reflect sent or received traffic on a particular port to another analyzer port. The Port Mirror function must be configured to select one port to which monitored traffic is forwarded, using the "mirror to" command (see "Set Mirror To Port" on page 176). The "mirror to" port is the port to which frames are reflected, and where the analyzer is located.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The port to be monitored is specified with the “mirror ingress” and/or “mirror egress” commands (see “Set Ingress Port(s) to be Mirrored” on page 176). More than one port may be reflected at the same time. The port can be set to mirror received (“ingress”) frames, transmitted (“egress”) frames, or both.

The switch supports mirroring of packets that are forwarded by Layer2 and/or Layer3 switching. The choice is managed through the “mirror mode” command (see “Set Mirror Mode” on page 175).

Frames sent and received by the on-board CPU can also be monitored by using the “mirror cpu” command (see “Enable or Disable CPU Mirror Mode” on page 175). The user specifies the port to which frames sent by the CPU into the switch fabric may be mirrored. This mode is useful for debugging transactions between clients and the switch services, such as DHCP, FTP, TFTP, etc.

Care should be taken not to overload the “mirror-to” port.

Ping

The Ping command is useful for verifying the connectivity between the CPC441x and another IP device. See “Ping” on page 177.

Traceroute

The Traceroute command is useful in debugging connectivity problems in a routed network. This command will determine the route being taken by packets destined to a particular IP address. If packets are not making it to their destination, this command will help determine how far they get and where the problem might be. See “Trace Route” on page 177.

Embedded Diagnostics

The embedded diagnostic functions of the CPC441x ensure virtually faultless operation both at initialization and continuously during switch operation. The in-system verification includes Power-On Confidence (POC) tests and two levels of online Integrity tests.

Power-On Confidence (POC) Tests

Power-On Confidence (POC) tests are diagnostic tests run when the CPC441x is booted. The POC test suite includes only those diagnostic tests that do not affect externally attached devices. When running POC tests, the CPC441x becomes available to the user within 150 seconds of a power-on or reset. All subsystems are included in the POC suite.

Watchdog Timer

A hardware watchdog timer is supported that will remove the CPC441x from service if it is not refreshed periodically by the CPU. This guards against CPU failure. If the watchdog timer expires, link will be deasserted on all external ports, and the CPC441x will be reset. The user can configure the board to reboot after a watchdog event or to remain off line.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The same function that services the Watchdog Timer also verifies the integrity of many fundamental software processes. These processes include:

- Packet Receive Task
- Address Learning
- Spanning Tree
- GARP
- Link Aggregation
- RIP
- OSPF
- VRRP
- HTTP Server
- SNMP
- IGMP Snooping
- Parameter Storage
- Rmon
- TFTP/FTP/DHCP Servers

If any of these tasks dies, then the Watchdog Task will suspend servicing the hardware timer. This will cause a Watchdog expiration and the switch will either go offline or reboot, depending on the 'Reboot-On-Watchdog' setting (see "Enable or Disable Reboot on Watchdog Timeout" on page 238).

Level One Online Integrity Tests

Level One online integrity tests are run on a continuous basis while the CPC441x is in service. Online integrity tests are enabled by default, but the CPC441x also provides a method to disable them (see "Online Integrity Test Configuration" on page 178).

The integrity tests continuously operate during execution of application code to detect hardware faults. Upon detecting a fault, the CPC441x can take itself out of service. All attached clients will lose link. (See "Online Integrity Test Configuration" on page 178.)

Level Two Online Integrity Verification

The software on the CPC441x continuously verifies its own proper operation. If a fault is detected (e.g., memory leak, failure from low level driver, etc.), the switch will report the error to a logging task. The messages sent to this task may be displayed on the console, written to a file, or sent to a remote host.

If Level Two Integrity Testing is enabled, in addition to logging a message, the switch will also cause the reporting task to exit. If the Watchdog Timer is enabled, then the Watchdog Service routine will detect the task exit, and will take the switch offline or reboot (see "Enable or Disable Reboot on Watchdog Timeout" on page 238).

Level Two Integrity testing is disabled by default, but may be enabled using the 'integrity leveltwo enable' command.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Fault State

The Fault State is entered on the following events:

- POC Failure
- Watchdog Expiration (may be due to Level Two Integrity Failure)
- Level One Integrity Failure
- SMB (IPMI) Command

If the Fault State is entered from POC Failure, the CPC441x will not boot the application, unless the user intervenes. An opportunity to continue booting despite the failure is presented via the console port.

If the Fault State is entered while running the application, the default action of the CPC441x is to automatically reboot. The user may also configure the board to remain off line (ports disabled), but still responsive to commands over the console. This mode helps prevent cycling reboots and is also typically used where a backup switch is available. In cases where a single switch is used, reboot is usually preferred.

In the Fault State, the following conditions exist:

- The FAULT LED on the faceplate of the CPC441x will be illuminated
- The HEALTHY# signal on the Compact PCIbus interface will be de-asserted if jumper settings allow
- The Switched Ethernet ports are held in reset

If the CPC441x is rebooted after entering the Fault State, without performing a power cycle, then the Fault LED will remain illuminated to indicate that the card had experienced a Fault and HEALTHY# will remain de-asserted. However, the switched ports are released from reset to allow the board to go back into service.

Once the Fault LED is illuminated, the CPC441x must be power-cycled, either by extraction or via BDSEL#, to turn off the LED and to allow HEALTHY# to be re-asserted.

One possible algorithm to follow is to configure the CPC441x to stay offline in case of a Fault. If a Fault State is entered, the Shelf Manager will see HEALTHY# de-assert and it can log the event or send a notification. The Shelf Manager can further determine if the board should be brought back into service automatically based on local policy. If it decides to bring the board back into service, then the Shelf Manager can toggle BDSEL# to clear the Fault State (and turn off the FAULT LED). The CPC441x will execute its power-on diagnostics as part of its boot process, and if there is a hard fault on the switch, it will re-enter the Fault State and the Shelf Manager can remove it from service.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

21



Lua Programming Language

Overview

The CPC441x has a programming language interface that allows customized operation of the switch. The programming language is based on the Lua extension programming language designed and implemented at TeCGraf, the Computer Graphics Technology Group of PUC-Rio (the Pontifical Catholic University of Rio de Janeiro in Brazil). TeCGraf is a laboratory of the Department of Computer Science. The authors can be contacted by e-mail at lua@tecgraf.puc-rio.br.

The Lua language provides almost any programming language elements available in a language such as Pascal or C. Lua programs can be pre-compiled, but the user interface to Lua on the CPC441x is restricted to Lua programs created by the user and then stored in source code form on the CPC441x file system. These programs may then be executed via the CLI `exec` command. The `exec` command passes the file to an on-board Lua interpreter. See “Execute a Script File” on page 208. These programs can also be executed by entering the file name of the Lua source file.

CPC441x Lua programs can use any of the standard Lua program elements, except Floating Point math functions.

The Lua language on the CPC441x is enhanced by the inclusion of a library of functions that provides access to CPC441x Events, Status, and Configuration. Any command available to the user via the CLI is available under Lua.

The key topics in this chapter include:

- “Syntax” on page 450
- “Examples” on page 450
- “CPC441x Lua Library API” on page 470

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Syntax

The syntax of Lua programs is documented in the Lua Reference Manual which may be downloaded from the CPC441x product page at the Performance Technologies web site, http://www.pt.com. It is also included on the CPC441x CD-ROM.

Examples

This section has examples of some Lua programs that demonstrate the power Lua provides.

rc.lua

The **rc.lua** file provided on the CPC441x is a Lua program that is always executed by the switch as it boots. This file can be changed by the user to modify the switch behavior during boot. This file may be enhanced to add features such as the following:

- Acquire the switch configuration from a remote file system.
- Programmatically determine the slot that the switch is located in and set the configuration appropriately.
- Install event detectors that will trigger the execution of other Lua programs when those events occur, etc.

The **rc.lua** file that is shipped with the CPC441x by default is shown here:

```
-------------------------------------------------------------------------
-- rc.lua
--
-- This file is processed whenever the CPC441x is booted. It may be modified
-- by the user to perform any extra system initialization particular to the
-- application.
--
-- This file is a Lua program. Lua is an embedded programming language
-- interpreter designed by the Computer Graphics Technology Group at the
-- Pontificial Catholic University of Rio de Janeiro, Brazil.
--
-- Refer to the CPC441x User Manual for details on the Lua Programming
-- Language.
-------------------------------------------------------------------------

-------------------------------------------------------------------------
-- Display the switch information
--
-- Function:   rc
-- Parameters: args - None
-- Return:     None
-------------------------------------------------------------------------
print ("")
print ("")
print ("")
print ("============================================================")
cli("switch display")
print ("============================================================")
print ("")
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
--------------------------------------------------------------------------
-- Add an event detector to handle the hot swap event.
--------------------------------------------------------------------------
-- If the hotswap script exists, fire it up
-- This will handle any shutdown activities and turn on the Hot Swap LED
if (exists("flash:/hotswap.lua") == nil) then
    if (addEvent("hot swap", "flash:/hotswap.lua") == nil) then
        print ("rc.lua: Cannot register Hot Swap Event")
    end
end
-- User Adds Code Here
--------------------------------------------------------------------------
```

This program displays the switch system information, including:

- sysName
- sysDescr
- sysContact
- sysLocation
- cpc4400CommonMiscProductName
- cpc4400CommonMiscSwVersion
- cpc4400CommonMiscHwVersion
- cpc4400SwitchIPMACAddr

After printing the switch information, the program determines if the **hotswap.lua** program exists, and if it does, it adds an event handler to execute this program if the ejector handle is unlatched. This example is described below. See “CPC441x Lua Library API” on page 470 for a description of the `addEvent()` function.

The user can add additional programming at the end to perform local startup functions.

hotswap.lua

This example uses the detection of the ejector handle being unlatched to invoke a Lua program. This program is registered with the “hot swap” event by the standard **rc.lua** script.

```
--------------------------------------------------------------------------
-- hotswap.lua
--
-- This file defines the process for shutting down a board for removal.
-- The actual shutdown code is customer specific and is left to the
-- individual customer to implement.
--
--------------------------------------------------------------------------

-- This is the location for the shutdown procedure.

-- Turn on the Hot Swap LED
local ctr
local ejectStatus

print("Ejector handle open, turning on LED")
if idbU32Set("ptiSystemManagement:ptiCommonSysHsLed", 0, 1) ~= nil
  then
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
  print("Failure to turn on Hot Swap LED")
end

for ctr = 1, 200, 1 do
    taskDelay(5 * sysClkRateGet())                          -- wait 5 seconds
    ejectStatus = sysGetEjectorSwitchStatus()               -- get current ejector
handle status

    if ejectStatus == -1 then                              -- only supported on CPC4416
        print("Ejector handle status is not supported.")
        break
    end

    if ejectStatus == 0 then
        print("Ejector handle is now locked, turning off LED.")
        if idbU32Set("ptiSystemManagement:ptiCommonSysHsLed", 0, 2) ~= nil
          then
          print("Failure to turn off Hot Swap LED")
        end
        return
    end

    if ejectStatus == 1 then
        print("Ejector handle is still unlocked.")          -- Is printing this line
200 times sufficient?
    end
end
```

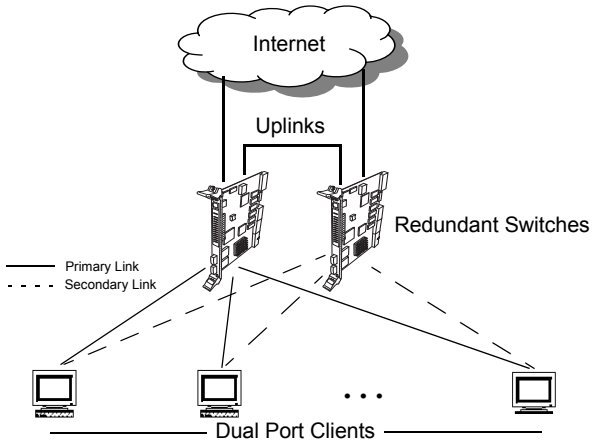
Any shutdown-specific commands should be added prior to turning on the Hot Swap LED.

genericLinkDetect.lua

This example may be used in a high-availability environment where two switches are used as redundant paths to a network for embedded nodes or clients. Each switch has one or more ports that are configured as ‘uplinks’ to an external network. The clients each have a link to both switches. One of the links will be ‘active’ at any time, and the other link will be a ‘backup’ link. If the link is broken on the active link, the client will then use the backup link. This type of redundant Ethernet network architecture is shown in Figure 21-1: “Redundant Ethernet Network Architecture”

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 21-1: Redundant Ethernet Network Architecture



If both uplink ports on the active switch were to fail, the clients would be disconnected from the external network. When connected to clients with redundant links, it may be useful to monitor the status of the uplink ports and force the clients to select the alternate switch when the uplink ports no longer provide a path to the external network.

This functionality may be provided through the use of the Lua program, **genericLinkDetect.lua**, described in this section. This program is provided as an example on the switch, but is not enabled by default. The user may use the example as a template, providing application-specific enhancements. The **rc.lua** script may then be modified to start the program to run on the switch whenever the switch is reset.

The **genericLinkDetect.lua** program illustrates the registration of a switch event with a Lua program. The example uses the detection of link change (up or down) on a switch port. The registered Lua program will execute each time a link change event is detected. The registration is performed within the script when it is called by **rc.lua** or executed manually. In these startup cases, the variable, portNumber, will be nil, and code will make the registrations. Thereafter, the code will be executed on link changes, but in these cases, portNumber will be set by the system to identify the port on which link changed. To start up the script manually, simply copy **genericLinkDetect.lua** to **flash:/genericLinkDetect.lua** and execute the script by typing, genericLinkDetect. To start the script from **rc.lua**, the following snippet can be added to **rc.lua**;

```
-- Kickstart Link Detector
if (exists("flash:/genericLinkDetect.lua") == nil) then
    dofile("flash:/genericLinkDetect.lua")
end
```

The **genericLinkDetect.lua** program starts out by detecting the model of switch (thus it is ‘generic’). It does this by looking at the rfc1213:sysDescription MIB Object. From this, it selects one of the port list table sets. There are three port list tables per switch model that define which ports are client links, which connect between switches (not used in the script), and which are uplinks. The user can modify these tables as needed. The script then registers itself to run on link changes. When the script is invoked on a link change, it evaluates whether links are available on any uplink port. If any uplink port has a link, then the client ports are enabled. If none of the uplink ports have link, then the client ports are disabled, causing the clients to use the alternate switch.

A listing of the Lua program, **genericLinkDetect.lua** follows:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
--------------------------------------------------------------------------
-- genericLinkDetect.lua
--
-- This file defines the process for dropping links on the client ports
-- when the CPSB Switch loses link on all uplink ports. Link is dropped on
-- all embedded client interfaces. This causes the clients to
-- switch over to the alternate CPSB Switch.
--
-- This program is an event handler for all link changes on the CPSB Switch.
-- It will be invoked for both link up and link down events.
--
-- This version of the linkdetect.lua script that was originally provided
-- with the CPC4400 is intended to work with any of the ethernet switches.
--
--------------------------------------------------------------------------

--------------------------------------------------------------------------
-- Sample port selection for the CPC440x
--------------------------------------------------------------------------
clientlist44xx  = { 1,  2,  3,  4,  5,  6,  7,  8,
                    9, 10, 11, 12, 13, 14, 15, 16,
                   17, 18, 19, 20, 21, 22, 23, 24 }
uplinks44xx     = { 25 }
intraswitch44xx = { 26 }

--------------------------------------------------------------------------
-- Sample port selection for the CPC5400
--------------------------------------------------------------------------
clientlist5400  = { 1,  2,  3,  4,  5,  6 }
uplinks5400     = { 7 }
intraswitch5400 = { 8 }

--------------------------------------------------------------------------
-- Sample port selection for the CPC660x
--------------------------------------------------------------------------
clientlist660x  = { 1,  2,  3,  4,  5,  6,  7,  8,
                    9, 10, 11, 12, 13, 14, 15, 16,
                   17, 18, 19, 20, 21, 22 }
uplinks660x     = { 23 }
intraswitch660x = { 24 }

-- define local variables with values useful to the program
UP = 1
DOWN = 2
TRUE = 1
LAST_UPLINK_STATE = 1 -- Index of User Variable for last state

-- Switch Board descriptions. Used to identify which board we have
sysNames =
       {
       ["Ethernet Switch SNMPv1/v2c/v3 Agent"]                 = "cpc4400",
       ["PTI CPC4400 Ethernet SNMPv1/v2c/v3 Agent"]            = "cpc4400",
       ["PTI CPC4400 24/2 Ethernet Switch SNMPv1/v2c/v3 Agent"] = "cpc4400",
       ["PTI CPC4401 24/2 Ethernet Switch SNMPv1/v2c/v3 Agent"] = "cpc4400",
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
       ["PTI CPC4406 24/2 Ethernet Switch SNMPv1/v2c/v3 Agent"] = "cpc4400",
       ["CPC4400 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc4400",
       ["CPC4401 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc4400",
       ["CPC4406 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc4400",
       ["CPC4411 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc4400",
       ["CPC4416 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc4400",
       ["CPC5400 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc5400",
       ["CPC6400 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc6400",
       ["CPC6600 Ethernet Switch SNMPv1/v2c/v3 Agent"]          = "cpc6600"
       }

clientTable =
    {
    ["cpc4400"] = clientlist44xx,
    ["cpc5400"] = clientlist5400,
    ["cpc6600"] = clientlist660x
    }

intraswitchTable =
    {
    ["cpc4400"] = intraswitch44xx,
    ["cpc5400"] = intraswitch5400,
    ["cpc6600"] = intraswitch660x
    }

uplinkTable =
    {
    ["cpc4400"] = uplinks44xx,
    ["cpc5400"] = uplinks5400,
    ["cpc6600"] = uplinks660x
    }

-- Extract the board type from the RCF1213 description
descr = idbOctetStringGet("rfc1213:sysDescr", 0, 255 )
switchMib = sysNames[descr]
if (nil == switchMib) then
    logMsg("Unexpected Switch Name returned\n")
    return
end

clientlist = clientTable[switchMib]
intraswitchlist = intraswitchTable[switchMib]
uplinklist = uplinkTable[switchMib]

if ((nil == clientlist) or (nil == intraswitchlist) or (nil == uplinklist)) then
    logMsg("Unexpected Switch Name returned\n")
    return
end

LinkAdmin   = format("%s:%sArchIfaceLinkAdmin",switchMib,switchMib)
IfaceLink   = format("%s:%sArchIfaceLink",switchMib,switchMib)
UsrVariable = format("%s:%sUsrVarInteger",switchMib,switchMib)

--------------------------------------------------------------------------------
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
-- Function: portInList
-- Parameters: Port, Table of Ports
-- Description: Return TRUE if the specified Port is in the List,
--      else return FALSE
--------------------------------------------------------------------------------
function portInList(port, portlist)
    local x = foreachi( portlist,
        function(i, v)
            if (%port == v) then
                return(TRUE)
            else
                return(nil)
            end
        end)
    if (nil == x) then
        return(FALSE)
    else
        return(TRUE)
    end
end

--------------------------------------------------------------------------------
-- Function: anyLinkUp
-- Parameters: Table of Ports
-- Description: Return UP if any switch port in the list is up,
--      else return DOWN
--------------------------------------------------------------------------------
function anyLinkUp(portlist)
    local x = foreachi( portlist,
        function(i, v)
            if ( UP == idbU32Get(IfaceLink, ("1." .. v)) ) then
                return(UP)
            else
                return(nil)
            end
        end)
    if (nil == x) then
        return(DOWN)
    else
        return(UP)
    end
end

--------------------------------------------------------------------------------
-- Function: setPortLinkStates
-- Parameters: Table of Ports, new state - UP or DOWN
-- Description: Set the port states in the table to the specified value
--------------------------------------------------------------------------------
function setPortLinkStates(portlist, state)
    foreachi( portlist,
        function(i, v)
            idbU32Set(LinkAdmin, ("1." .. v), %state)
        end)
end
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
-------------------------------------------------------------------------
-- This is the code entry point upon change in link status on a port.
-- The port number is 'passed' to us in portNumber. This is nil when called
-- from rc.lua or command line. If the link change is on an uplink port, then
-- evaluate whether to assert or drop links on the client ports.
-------------------------------------------------------------------------
if (nil == portNumber) then
    logMsg(format("Initialize Link Detector for %s\n", switchMib))
    -------------------------------------------------------------------------
    -- Register link handlers
    -------------------------------------------------------------------------
    if (nil ~= exists("flash:/genericLinkDetect.lua") ) then
        logMsg("Location of genericLinkDetect.Lua is unknown\n")
        return
    end
    if (addEvent("link up", "flash:/genericLinkDetect.lua") == nil) then
        logMsg("genericLinkDetect.lua: Cannot register Link Up Detector\n")
    end
    if (addEvent("link down", "flash:/genericLinkDetect.lua") == nil) then
        deleteEvent("link up")
        logMsg("genericLinkDetect.lua: Cannot register Link Down Detector\n")
        return
    end

    -------------------------------------------------------------------------
    -- Initialize current state
    -------------------------------------------------------------------------
    if (UP == anyLinkUp(uplinklist)) then
        setPortLinkStates(clientlist, UP)
        idbU32Set(UsrVariable, LAST_UPLINK_STATE, UP)
    else
        setPortLinkStates(clientlist, DOWN)
        idbU32Set(UsrVariable, LAST_UPLINK_STATE, DOWN)
    end
end

-------------------------------------------------------------------------
-- Process link status changes
-- If the port that changed is an uplink port, then get link status of all
-- uplinks. If status is 'any link up' and we were DOWN, then go UP. If
-- all uplinks are down and we were UP, go DOWN.
-------------------------------------------------------------------------
if (portInList(portNumber, uplinklist)) then
--  print(format("Uplink port %d Changed\n", portNumber))
    lastState = idbU32Get(UsrVariable, LAST_UPLINK_STATE)
    currentState = anyLinkUp(uplinklist)
--  print(format("last=%d, current=%d\n", lastState, currentState))
    if ((DOWN == lastState) and (UP == currentState)) then
        logMsg("Uplink Up, Enable Clients\n")
        setPortLinkStates(clientlist, UP)
        idbU32Set(UsrVariable, LAST_UPLINK_STATE, UP)
    elseif ((UP == lastState) and (DOWN == currentState)) then
        logMsg("Uplink Down, Disable Clients\n")
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
            setPortLinkStates(clientlist, DOWN)
            idbU32Set(UsrVariable, LAST_UPLINK_STATE, DOWN)
        end
    end
```

Using Lua Programs to Manage Configurations

The CPC441x allows a high level of user configuration. Once a switch has been in service and configured to support a particular application, the configuration information can be stored in a safe place. The configuration can then be downloaded to a switch and installed and run as needed.

The two examples in this chapter (**savecfg.lua** and **recovercfg.lua**) demonstrate the use of Lua programs to automatically save a CPC441x configuration to a remote file system and then to automatically recover the last saved configuration information at boot time. These programs are also useful for replicating the configuration of a failed switch onto its replacement.

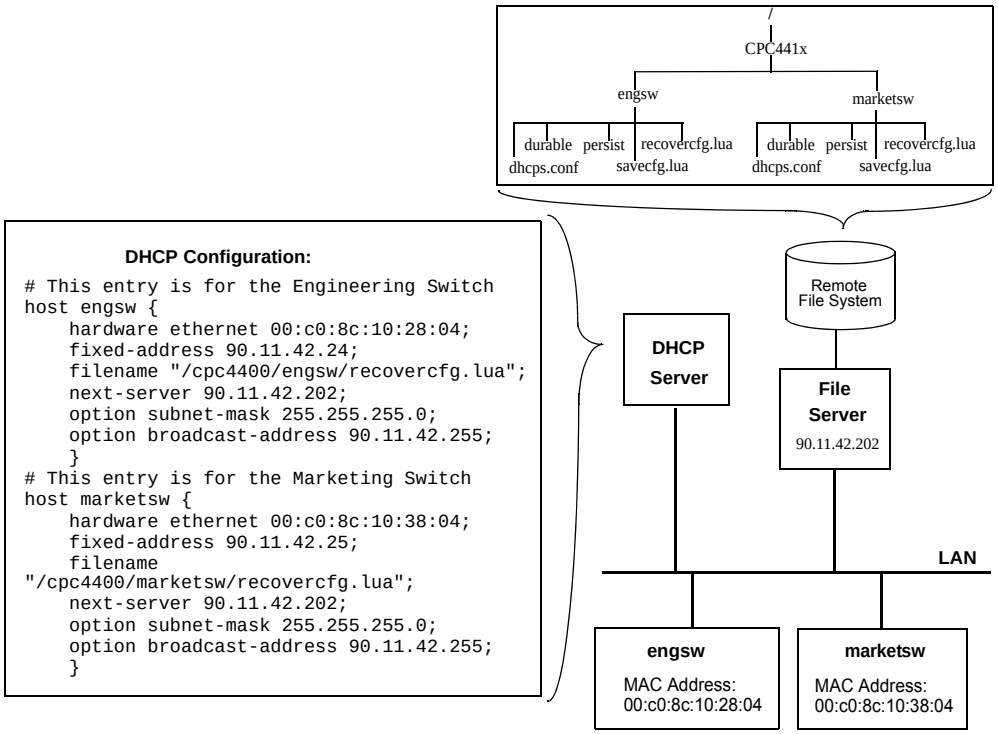
Both programs assume the use of DHCP to provide the CPC441x IP address, the address of a File Server, and the name of a configuration file. When the CPC441x is a DHCP client, the server may provide a file to the CPC441x which will be interpreted as a Lua program. The CPC441x will transfer this file with TFTP when it receives the DHCP lease, and will execute it. In these examples, the configuration file provided by DHCP is **recovercfg.lua**. Executing this program makes the CPC441x recover its configuration from the remote file system.

In order to support multiple CPC441xs on the network using a single file server, the user may wish to provide a directory on the server for each card. Each directory will contain the configuration file for the associated CPC441x. For example, assume that there are two CPC441xs on the network. One is used for engineering and one for marketing. They have different configurations. The user configures the DHCP server to provide an IP Address to each based on the MAC Address of the switch and to provide a path to a configuration file.

The configuration details depend on the DHCP Server. The following diagram illustrates a potential network, and shows a DHCP Server and File Server. The DHCP configuration shown is in the syntax of a Linux Hosted DHCP server. This configuration would have to be provided in the proper syntax for your particular DHCP server.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 21-2: Automated Configuration Example



The DHCP Server is configured to provide the address of the File Server (through the `siad` parameter), and the path to the CPC441x configuration file (through the `file` parameter). The configuration file is **recovercfg.lua**. The file parameter points to a different subdirectory on the File Server for each of the switches. This is because each switch will have different settings and the settings will be stored in files of the same name (**durable**, **persist**, etc.), but in different directories. The **savecfg.lua** program, shown below, will extract the directory name from the DHCP-provided `file` parameter to determine where to save the switch's configuration files. The **savecfg.lua** file is stored in these directories and is propagated to the switches by **recovercfg.lua**.

savecfg.lua

Whenever the switch settings are saved to flash, they are stored in one of two files: **durable**, or **persist**. The user can manually copy these files to a remote filesystem whenever they change. Alternatively, the user can write a Lua program to automatically perform the copy. The Lua program, **savecfg.lua** is an example of how this might be done.

This program relies on a "configuration save" event that may be registered to invoke the program by a save to flash. This registration is performed by the **recovercfg.lua** program described below. The 'configuration save' event detector passes an argument to the registered Lua program, to indicate which file was changed. This argument is passed in a variable called `fileName`. This parameter is used to determine which file to send to the remote filesystem.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

The **savecfg.lua** program listing follows:

```
------------------------------------------------------------------------
-- savecfg.lua
--
-- This file defines the process for saving a configuration change made
-- to the CPC441x to a remote filesystem. An event detector is
-- installed to detect when any changes to the NVM files (persist or durable)
-- are saved to flash. When the event occurs, this program is executed.
--
-- The IP address of the remote filesystem is determined in this case
-- by refering to the Server Address ID (siad). This is the IP
-- Address of the File System server provided by the DHCP Server when
-- the CPC441x booted. Each time this program runs, the context is
-- brand new and disappears when the program completes, so the IP
-- Address must be determined each time we run.
------------------------------------------------------------------------

-- Get the path to this card's configuration file provided by DHCP.
-- This will likely be unique for each CPC441x in the network.
file = idbOctetStringGet("cpc4400:cpc4400CommonMiscDHCPClientFile", 0, 255 )

-- Extract my card's directory path from the DHCP provided path to my
-- configuration file. This is done by extracting from the 'file' string
-- the characters up to the last '/'. If there are no '/' characters in
-- the 'file' string, then my configuration file is apparently at the
-- TFTP Server Root directory. In this case, set serverDir to null.
serverDir = gsub (file, "^(.+)/(.+)$", "%1")
if (serverDir == file) then
    serverDir = ""
end

-- get the changed file’s base name without the mount point
changedFile = gsub (fileName, "flash:", "")

-- Set the IP Address of the file server
serverIP = format("%d.%d.%d.%d",
    str2ip(idbOctetStringGet("cpc4400:cpc4400CommonMiscDHCPClientSIAD", 0, 4)))

-- If server is alive, send my settings to him
print(format("savecfg.lua: File %s has changed, check Server", fileName))
if ping( serverIP, 1 ) == nil then
    print(format("savecfg.lua: %s is being saved to %s", fileName, serverIP))
    -- Server is alive, copy the NVM files to him
    if (tftp("put", serverIP, fileName, serverDir .. changedFile) ~= nil) then
        print ("savecfg.lua: tftp put error")
    else
        print ("Done")
    end
else
    print("savecfg.lua: Server is not accessible, can't save settings")
end
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

When **savecfg.lua** is invoked, it determines the IP Address of the File Server by getting the MIB variable, `cpc4400CommonMiscDHCPClientSIAD`. This is the File Server Address provided to the CPC441x by DHCP when the CPC441x booted. The program checks the availability of the Server by "pinging" it. If the Server is available, the changed file is sent to it using TFTP.

The file is sent to the directory where the DHCP provided configuration file came from. This is determined by extracting the directory portion of the `cpc4400CommonMiscDHCPClientFile` parameter.

Note: *Since the settings are transferred using TFTP-put, the server may need to have a file with the name* ***durable*** *and/or* ***persist*** *having global write permissions in the directory that is being written to.*

recovercfg.lua

This example illustrates a Lua program that allows a replacement CPC441x to recover its settings from a File Server when it is installed. It assumes the use of DHCP to provide a lease address, the address of the File Server, and the path to the **recovercfg.lua** file. When the new CPC441x is powered on, it will use DHCP to acquire the lease and download the **recovercfg.lua** file.

The **recovercfg.lua** program first defines some directories in which to operate. The server directory for the board is extracted from the *file* parameter provided by the DHCP server. Two directories are defined in ramdisk to use for temporary storage; backup and restore. The backup directory will be used to store any Flash files that are going to be over-written. They will be restored to Flash if an error occurs during the recovery process. The restore directory is used to download the server files into before writing them to Flash.

The list of files that are recovered by this program are defined in a table. The program will attempt to backup each listed file from Flash, download each file from the server to the restore directory, compare the Flash version of each listed file to those downloaded, and save the downloaded files to Flash if they differ from the server's version.

Note that the list of files recovered from the file server should include all files that define the configuration of the board. In this example, these include: **durable** and **persist**, and also the dhcps.conf file, **savecfg.lua**, and **rc.lua**. The **durable** and **persist** files represent the MIB settings. The other files are supporting files managed directly by the user. The user should include all files that reflect the CPC441x configuration in the recoverFiles table (see Lua listing below).

The **durable** and **persist** files may be automatically saved if they are changed, since the CPC441x generates an event when these change. User files must be manually saved on the fileserver if they are changed.

The program defines several functions used by the recovery process:

- cleanUpRecover() - This function will clean up the temporary ramdisk files and directories after the recovery process.
- backupFile() - This function will save the flash files that are to be over-written, so they may be restored if a failure occurs.
- restoreFiles() - This function restores the backup files if an error occurred.
- getServerFiles() - This function gets the server files and puts them in ramdisk.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- installFiles() - This function compares the downloaded server files to the versions in Flash. If they differ, this function over-writes the flash version with the server version. If the **durable** or **persist** files differ, the CPC441x must be rebooted to ensure that all parameters are in effect.

After defining the functions and variables, the program falls into its main thread. The main thread performs the following steps:

- Create the temporary ramdisk directories
- Back up the Flash files
- Get the server files
- Install the server files
- Install and run the new **durable** file with the recover() function (see “CPC441x Lua Library API” on page 470)
- Clean up the temporary files
- Install the **savecfg.lua** program as the “data save nvm” event handler so that future changes to the board’s settings will be stored on the file server

The **recovercfg.lua** listing follows:

```
--------------------------------------------------------------------------
-- recovercfg.lua
--
-- This file defines the recovery process. It is put in place by the user
-- and specifies which files to recover from the server and how to instantiate
-- them.
--
-- It depends on the use of DHCP to acquire the IP address of the File
-- Server and (potentially the path to this file).
--
-- The process is;
--    Create backup directory called ‘backup’ in ramdisk
--    Copy local files to ramdisk:/backup in case of error
--    Create temp directory called ‘recover’ in ramdisk
--    Copy all files from the server to ramdisk:/recover
--    If the copied files are different from the local files,
--        over-write the local file
--    If error occurs, restore backed up files
--
--------------------------------------------------------------------------

-- Set debugOn to any non-nil value to display debug messages
debugOn = 1
need2reset = nil

-- Get the path to this card’s configuration file provided by DHCP.
-- This will likely be unique for each CPC441x in the network.
file = idbOctetStringGet(“cpc4400:cpc4400CommonMiscDHCPClientFile”, 0, 255 )

-- Extract my card’s directory path from the DHCP provided path to my
-- configuration file. This is done by extracting from the ‘file’ string
-- the characters up to the last ‘/’. If there are no ‘/’ characters in
-- the ‘file’ string, then my configuration file is apparently at the
-- TFTP Server Root directory. In this case, set serverDir to null.
serverDir = gsub (file, “^(.+)/(.+)$”, “%1”)
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
if (serverDir == file) then
    serverDir = “”
end
if (debugOn) then
    print(format(“serverDir=%s”, serverDir))
end

-- set directories names in which to operate
flashDir   = “flash:”
backupDir  = “ramdisk:/backup”
recoverDir = “ramdisk:/recover”

-- Set the IP Address of the file server
siad = idbOctetStringGet(“cpc4400:cpc4400CommonMiscDHCPClientSIAD”, 0, 4)
serverIP = format(“%d.%d.%d.%d”, str2ip(siad))

-- Table of files to recover
recoverFiles = {
      “/persist”,
      “/durable”,
      “/savecfg.lua”,
      “/runtime.lua”,
      “/dhcps.conf”,
      “/rc.lua”
}

-- clean up ramdisk after recover
function cleanUpRecover()
    -- clean up the temp directory, if it exists
    foreach (recoverFiles,
            function(i, v)
                -- generate full path name of recover file in ramdisk
                local cleanFile = (recoverDir .. v)
                -- generate full path name of backup file
                local backupFile = (backupDir .. v)
                -- remove the file the temp directory
                if (debugOn) then
                    print(format(“cleanUpRecover: Remove %s and %s”, cleanFile,
backupFile))
                end
                remove (cleanFile)
                remove (backupFile)
                return (nil)
            end )
    -- remove the directories
    if (debugOn) then
        print(format(“cleanUpRecover: Remove %s”, recoverDir))
    end
    remove (recoverDir)
    if (debugOn) then
        print(format(“cleanUpRecover: Remove %s”, backupDir))
    end
    remove(backupDir)
end
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
-- backup the current copies of all files that may be over-written
function backupFiles()
    return (foreach(recoverFiles,
            function(i, v)
                -- copy the flash file to the backup directory, return result
                if (debugOn) then
                    print (format("backupFiles: Copying %s to %s", (flashDir .. v),
(backupDir .. v)))
                end
                -- if the file exists in flash, back it up
                if (exists((flashDir .. v)) == nil) then
                    return (copy((flashDir .. v), (backupDir .. v) ))
                else
                    return(nil)
                end
            end ))
end

-- restore the original copies of all files
function restoreFiles()
    return (foreach(recoverFiles,
            function(i, v)
                -- copy the backup files to the flash files, return result
                if (debugOn) then
                   print (format("restoreFiles: Copying %s to %s", (backupDir .. v),
(flashDir .. v)))
                end
                -- if the file exists in backupDir, restore it
                if (exists((backupDir .. v)) == nil) then
                    return (copy((backupDir .. v), (flashDir .. v)))
                else
                    return(nil)
                end
            end ))
end

-- get the recover files from the server
function getServerFiles()
    -- get the 'from' files into recoverDir
    return (foreach (recoverFiles,
            function(i, v)
                 if (debugOn) then
                     print(v)
                 end
                 -- concatenate the recover directory and the filename
                 local getFile = (recoverDir .. v)
                 if (debugOn) then
                     print(getFile)
                 end
                 -- concatenate the server directory and the filename
                 local serverFile = (serverDir .. v)
                 if (debugOn) then
                     print(serverFile)
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
                end
                -- get the server file to the recover directory, return result
                if (debugOn) then
                     print (format("TFTP Transfer from %s:%s to %s", serverIP,
serverFile, getFile))
                end
                return (tftp("get", serverIP, serverFile, getFile))
           end ))
end

-- install the recovered files
function installFiles()
    return (foreach(recoverFiles,
           function(i, v)
                -- concatenate the recover directory and the filename
                local installFile = (recoverDir .. v)
                   -- concatenate the flash directory and the filename
                   local flashFile = (flashDir .. v)
                   if (cmp (installFile, flashFile) == nil) then
                       if (debugOn) then
                          print (format("installFiles: No copy of %s", installFile))
                       end
                       return(nil)
                   end
                   -- copy the temp file to the 'to' file, return result
                   if (debugOn) then
                       print (format("installFiles: Copying %s to %s", installFile,
flashFile))
                   end
                   if ((v == "/durable") or (v == "/persist")) then
                       need2reset=1
                   end
                      return (copy(installFile, flashFile))
              end ))
end

--------------------------------------------------------------------------
-- Here's the recover process executed in-line by rc.lua
--------------------------------------------------------------------------
print (format("Recovering from %s", serverIP))

-- make the necessary directories
-- ignore errors at this point, the directories may already exist
mkdir(recoverDir)
mkdir(backupDir)

-- back up the flash files
backupFiles()

-- get the recover files from the server
if (getServerFiles() ~= nil) then
    print("Error getting files. Recover Aborted")

-- Install files
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
elseif (installFiles() ~= nil) then
    print(“Error Installing files. Recover Aborted”)

-- Instantiate the settings
elseif (need2reset ~= nil) then
    print(“Durable/Persist Changed. Need to Reboot...”)
    cli(“sleep 5”)
    cli(“switch reset”)

else
    -- clean up ramdisk
    if (debugOn == nil) then
         cleanUpRecover()
    end
    print(“Recover Successful”)
    -- fire up the savecfg.lua program
    -- This will cause my settings to be saved on the server when they change
    if (addEvent(“data save nvm”, “flash:/savecfg.lua”) == nil) then
         print (“recovercfg.lua: Cannot register NVM Save Event”)
    end
end
```

Managing Automated Configuration

In order to take advantage of the **savecfg.lua** and **restorecfg.lua** programs, the following guidelines should be observed:

- Before placing a CPC441x into service, note its MAC Address located on the board label.
- If the board is new, create a directory on the File Server with the files that are to be managed. You may want to have a factory version of **durable** and dhcps.conf available to populate the directory. The **rc.lua**, **savecfg.lua** and **recovercfg.lua** programs should be modified according to your needs and stored in the new directory. Update the DHCP Server configuration file to support the new card.
- If the board is a replacement, the directory should already be in place and you only need to change the MAC Address in the DHCP configuration file.
- Ensure that DHCP is enabled on the card.

User-Defined Trap Test

Following is a sample Lua script setting up the User-Defined trap test:

```
----------------------------------------------------------------
--      FILE: User Defined Trap Test
----------------------------------------------------------------

dofile("common.lua")

row_status_types = { "active", "notInService", "notReady", "createAndGo",
"createAndWait", "destroy" }

data_types = { "string-value", "integer-value" }
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
-----------------------------------------------------------------
--      Create/Send a trap with index 1 and string "test one"
-----------------------------------------------------------------

local trapid = format( "%d", 1)

    val = idbU32Set("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus",
                    trapid,
                    getTableIndex(row_status_types, "createAndWait"))

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus create
failed\n"))
    end

    val = idbOctetStringSet("ptiSystemManagement:ptiCommonUserDefinedTrapString",
trapid,"test one" )

    if ( val ) then
       print(format("set ptiSystemManagement:ptiCommonUserDefinedTrapString
failed\n"))
    end


    val = idbU32Set("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus",
                    trapid,
                    getTableIndex(row_status_types, "active"))

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus active
failed\n"))
    end

-----------------------------------------------------------------
--      Create/Send a trap with index 2 and string "test two"
-----------------------------------------------------------------

local trapid = format( "%d", 2)

    val = idbU32Set("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus",
                    trapid,
                    getTableIndex(row_status_types, "createAndWait"))

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus create
failed\n"))
    end

    val = idbOctetStringSet("ptiSystemManagement:ptiCommonUserDefinedTrapString",
trapid,"test two" )

    if ( val ) then
       print(format("set ptiSystemManagement:ptiCommonUserDefinedTrapString
failed\n"))
    end
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
    val = idbU32Set("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus",
                    trapid,
                    getTableIndex(row_status_types, "active"))

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus active
failed\n"))
    end


----------------------------------------------------------------
--     Add another varbind to trap that has index 1
--     When adding a varbind - you must specify the objects
--     identifier with the instance, like example below 'varbindoid'
--     and call the user defined trap lua-helper 'idbObjIdAnySet'
--     with the 'varbindoid' and the oid_length and instance_length
--     for arguments - like in example below...
----------------------------------------------------------------



local trapid = format( "%d", 1)
local varbindid = format( "%d", 3)
local entryid = format("%d.%d",trapid,varbindid)
local varbindoid = "1.3.6.1.2.1.2.2.1.8.17825793"

    val = idbU32Set("ptiSystemManagement:ptiCommonUserDefinedTrapVarBindRowStatus",
entryid, getTableIndex(row_status_types, "createAndWait"))

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapVarBindRowStatus
create failed\n"))
    end

   val = idbOctetStringSet("ptiSystemManagement:ptiCommonUserDefinedTrapObjectName",
entryid,"rfc1213:ifOperStatus" )

    if ( val ) then
       print(format("set ptiSystemManagement:ptiCommonUserDefinedTrapObjectName
failed\n"))
    end

    val = idbObjIdAnySet("ptiSystemManagement:ptiCommonUserDefinedTrapVariable",
                     entryid,varbindoid,10,1 )

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapVariable failed\n"))
    end


    val = idbU32Set("ptiSystemManagement:ptiCommonUserDefinedTrapDataType",
entryid,getTableIndex(data_types, "integer-value" ))

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapDataType failed\n"))
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
    end

--
-- You can set this next object to 'active' as many times as you want to send this
trap
--
    val = idbU32Set("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus",
trapid,getTableIndex(row_status_types, "active"))

    if ( val ) then
       print(format("ptiSystemManagement:ptiCommonUserDefinedTrapRowStatus active
failed\n"))
    end
```

Walking Static Route Table with Lua - walkStaticRoutes.lua

When performing an idbU32GetNext on "cpc4400:cpc4400L3IpStaticRowStatus" it will return the value "0.0.0.0" if there is a default gateway configured. If you were to simply loop until idbU32GetNext returned nil, the script would be stuck in an infinite loop. This is an example of the correct way to iterate through all of the static route entries.

```
-------------------------------------------------------------------------
-- walkStaticRoutes.lua
--
-- This script demonstrates the proper method of iterating through all
-- of the static routes on the system
--
-------------------------------------------------------------------------
local r_val;
local r_index = "0.0.0.0";

-- special case for default gateway entry
if idbU32Get("cpc4400L3Mib:cpc4400L3IpStaticRowStatus", "0.0.0.0" ) then
    print("static route default gateway entry '0.0.0.0'");
    r_index = "0.0.0.1"
end

repeat
    r_val, r_index = idbU32GetNext("cpc4400L3Mib:cpc4400L3IpStaticRowStatus", r_index
);
    if ( r_val==1 ) then
       print(format("static route entry '%s'", r_index));
    end
until r_val == nil
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

CPC441x Lua Library API

This section describes the API to the CPC441x extensions to the Lua language. The functions that come with Lua are documented in the Lua manual and are not repeated here.

Table 21-1: “CPC441x Lua Programming Library” provides an alphabetical list of the library functions added to support the CPC441x.

Table 21-1: CPC441x Lua Programming Library

Function Name	Description	Reference
addEvent()	Register a Lua program to run upon the occurrence of an event.	Page 472
arpAdd()	Add an entry for specified IP address mapped to specified MAC address.	Page 475
arpDelete()	Delete the entry for the specified IP address.	Page 476
band()	Bit-wise AND Function.	Page 484
bor()	Bit-wise OR Function.	Page 484
bnot()	Bit-wise NOT Function.	Page 484
bxor()	Bit-wise XOR Function.	Page 484
cli()	Execute a CLI command from within a Lua program.	Page 484
cmp()	Compare two files for equality.	Page 473
copy()	Copy a file.	Page 473
deleteEvent()	De-register a Lua program previously registered to run upon the occurrence of an event.	Page 472
exists()	Test for the existence of a file.	Page 473
filesize()	Display size of specified file.	Page 474
freespace()	Display amount of free space in specified device.	Page 474
ftp()	Use FTP to transfer a file.	Page 474
getdir()	Build a Lua table from the contents of a directory.	Page 472
idbObjIdAnySet()	Set an Object Identifier variable.	page 479
idbOctetStringGet()	Get an Octet String type IDB object.	Page 480
idbOctetStringGetNext()	IDB string object Get Next function.	Page 480
idbOctetStringSet()	Set the value of an Octet String IDB Object.	Page 480
idbU32Get()	Get an unsigned 32-bit IDB object value.	Page 478
idbU32GetNext()	IDB U32 object Get Next function.	Page 478
idbU32Set()	Set the value of a 32-bit unsigned IDB Object.	Page 479
imod()	Integer Modulus Function.	Page 484
inputChar()	Display character typed at STDIN device.	Page 477

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 21-1: CPC441x Lua Programming Library *(Continued)*

Function Name	Description	Reference
ip2str()	Convert a Lua string formatted as 4 dot-separated decimal integers into an IDB variable that represents an IP Address (octet string).	Page 483
lnameToOid()	Similar to 'nameToOid' but the length of the string is also added to the beginning of the returned OID value.	Page 482
logMsg()	Log a message to the console.	Page 484
mac2str()	Convert a Lua string formatted as 6 colon separated hex integers into an IDB variable that represents a MAC Address (octet string).	Page 483
mkdir()	Make a directory.	Page 473
nameToOid()	Provides a dot-separated decimal representation of the ASCII string that spells the name of the object.	Page 482
ping()	Test connectivity to a host using ICMP ECHO.	Page 484
readline()	Output specified prompt at the STDOUT device and return characters typed at STDIN device up to a newline.	Page 477
rename()	Rename a file.	Page 474
setDate()	Set the date.	Page 476
setDateAndTime()	Set the date and time.	Page 476
setTime()	Set the time.	Page 476
shiftl()	Bit-wise LEFT Shift Function.	Page 483
shiftr()	Bit-wise RIGHT Shift Function.	Page 483
str2mac()	Convert an IDB variable that represents a MAC Address (octet string) to a set of 6 byte values.	Page 483
sysClkRateGet()	Display number of system timer clicks per second.	Page 477
sysGetEjectorSwitchStatus()	Check the ejector handle status.	Page 485
taskDelay()	Delay calling task for specified number of clicks.	Page 477
tftp()	Use TFTP to transfer a file.	Page 475

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Event Management

Add an Event Handler

`addEvent (event, function)`

Installs a function to execute upon the occurrence of an event.

`event` is a string set to one of the names in Table 5-6: “Event Names and Descriptions” on page 96.

`function` The function argument is a path to a Lua program that will execute upon the occurrence of the event. Returns nil upon success, otherwise failure.

Example

```
print (addEvent (“data save nvm", “flash:/savecfg.lua”) )
```

Remove an Event Handler Registration

`deleteEvent (event)`

Removes the registration of the function to execute upon the occurrence of an event.

`event` is a string set to one of the values listed under `addEvent()` above. Returns nil upon success, otherwise failure.

Example

```
print (deleteEvent (“data save nvm") )
```

File System Management

Generate Lua table from directory contents

`getdir (directory)`

Generates a table of entries from the files located in the specified directory. This can be used to programmatically perform an operation on all files in a directory.

`directory` is a string set to the directory name.

Return Values

The return value is a Lua table of the file names, with one entry for each file found.

Example

```
foreach (getdir("flash:/"),
    function(v, i)
        print (format("%s", v))
    end
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Compare files

`cmp (file1, file2)`

Compare the files, file1 and file2. If they are identical, returns nil.

`file1` and `file2` are strings set to the paths of the two files.

Example

```
if (cmp (“flash:/durable”, “ramdisk:/durable”) == nil) then
    print (“The files are the same”)
else
    print (“The files differ”)
end
```

Copy files

`copy (file1, file2)`

Copy the file, file1 to the file, file2. Return nil if successful.

Example

```
print (copy (“flash:/durable”, “ramdisk:/durable”))
```

Make a directory

`mkdir (directory)`

Creates a directory named as specified.

where

`directory` is a string set to the name of the directory to create. Returns nil if successful.

Example

```
print (mkdir (“flash:/temp”) )
```

Check for existence of file

`exists (file)`

Returns nil if the file specified exists.

Example

```
if (exists (“flash:/durable”) == nil) then
    print (“File exists”)
else
    print (“File does not exist”)
end
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Check for size of a file

`filesize (file)`

Returns the size in bytes of the specified file, or nil if the file specified does not exist.

Example

```
size = filesize (“flash:/durable”)
if (size == nil) then
    print (“File does not exist”)
else
    print (format (“File size is %d”, size))
end
```

Get the number of bytes available on a specified File System

`freespace (device)`

Returns the amount of free space in bytes of the specified storage device, or nil if the device specified does not exist.

Example

```
print (format (“Free Space on Flash is %d”, freespace(“flash:”))
```

Rename a File

`rename (file1, file2)`

Renames a file. **file1** is renamed **file2**.

Example

```
rename(“flash:/oldname”, “flash:/newname”)
```

File Transfer

Use FTP to transfer a file

`ftp (command, host, source, destination, user, password)`

Transfer a file between the CPC441x and a remote host.

`command`	is a string set to “get” to get a file from the remote host, or “put” to put a file.
`host`	is a string which provides the IP Address of the host in dotted decimal notation.
`source`	is a string set to the name of the source file.
`destination`	is a string set to the name of the destination file.
`user`	is the user name to use for access to the remote host.
`password`	is the password used to validate the user’s access to the remote host.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

User and password must be provided. If either argument is not provided, the FTP program will prompt the user for the missing argument(s). Since this is being used inside of a Lua program, there is no interactive shell.

Returns nil upon success.

Example

```
if ( ftp (“get”, “147.139.1.215”, “durable”, “ramdisk:/durable”,
“user1”, “password1”) == nil) then
    print (“Transfer successful”)
else
    print (“Transfer failed”)
end
```

Use TFTP to transfer a file

`tftp (command, host, source, destination)`

Transfer a file between the CPC441x and a remote host.

`command`	is a string set to “get” to get a file from the remote host, or “put” to put a file.
`host`	is a string which provides the IP Address of the host in dotted decimal notation.
`source`	is a string set to the name of the source file.
`destination`	is a string set to the name of the destination file.

Returns nil upon success.

Example

```
if ( tftp (“get”, “147.139.1.215”, “durable”, “ramdisk:/durable”) ==
nil) then
    print (“Transfer successful”)
else
    print (“Transfer failed”)
end
```

ARP Cache Access

The following section describes functions to add and remove entries from the ARP Cache.

Add an ARP Entry

`arpAdd(ip, mac, published)`

Adds an entry for the specified IP Address mapped to the specified MAC Address.

`ip`	is a quoted string in dot-decimal format.
`mac`	is a quoted string in colon-separated hexadecimal format.
`published`	is a boolean that indicates whether the switch should answer ARPs for the address.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Example
```
arpAdd(“192.168.1.1”, “00:c0:8c:00:00:00”, 0)
```

Remove an ARP Entry

`arpDelete(ip)`

Deletes the entry for the specified IP Address.

`ip` is a quoted string in dot-decimal format.

Example
```
arpDelete(“192.168.1.1”)
```

Clock and Timer Functions

The following section describes functions to manipulate Date and Time, and to access low level timer functions.

Set the Date

`setDate(date)`

Sets the date to the value specified.

`date` is a string in the format, “mm/dd/yyyy”.

Example
```
setDate(“12/25/2000”)
```

Set the Time

`setTime(time)`

Sets the time to the value specified.

`time` is a string in the format, “HH:MM:SS”.

Example
```
setTime(“12:00:00”)
```

Set the Date and Time

`setDateAndTime(time, date)`

Sets the date and time to the values specified.

`time` is a string in the format, “HH:MM:SS”.

`date` is a string in the format, “mm/dd/yyyy”.

Example
```
setDateAndTime(“12:00:00”, “12/25/2000”)
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Get the System Clock Rate

`sysClkRateGet()`

Returns the number of system timer ticks per second. Use ticks for taskDelay().

Example

```
ticks = sysClkRateGet()
```

Delay Task Processing

`taskDelay(ticks)`

Delays the calling task for the specified number of ticks. This function may be useful in Lua Event Handler scripts. The Event Handler script is executed as a task under vxWorks.

Example

```
taskDelay(ticks)
```

Console Input Functions

Input a Character

`inputChar()`

Returns the character typed at the STDIN device.

Example

```
ch = inputChar()
```

Input a Line

`readline(prompt)`

Outputs the specified prompt at the STDOUT device and returns the characters typed at the STDIN device up to a newline.

Example

```
answer = readline(“Enter the answer here: “)
```

Information Database Access

The Information Database (IDB) is the database of all managed objects on the CPC441x. The following commands are used to access and modify the CPC441x configuration from a Lua program.

All of the functions require an object name and an index. The set function also requires a value.

The object name used by the IDB access functions is a string set to the base name of the MIB file concatenated with the leaf node of the MIB path for the object.

For example, the MIB path for the `sysDescr` object is:

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
.iso.org.dod.internet.mgmt.mib-2.system.sysDescr
```

The leaf node is simply `sysDescr`. The MIB file that this parameter is located in is **rfc1213.mib**. The base name of this file is **rfc1213**. Therefore, the object name for this parameter is, **rfc1213:sysDescr**.

The index value is 0 for all scalar objects and is the appropriate index for tables of objects.

Get an Unsigned 32-bit Scalar IDB Object

`idbU32Get(object, index)`

Return the value of the IDB object.

`object` is a string set to the IDB object name.

`index` is a string set to the MIB table index. If an error occurs on the get, nil is returned.

Example

```
port2link = idbU32Get("cpc4400:cpc4400ArchIfaceLink", "1.2")
if (port2link == 1) then
    print (“Port 2 link is up”)
elseif (port2link == 2) then
    print (“Port 2 link is down”)
else
    print (“Error getting link status”)
end
```

IDB U32 Object Get Next

`idbU32GetNext (object, index)`

Return the index and the value of the next IDB object in a table of U32 objects.

`object` is a string set to the IDB object name

`index` is a string set to the MIB table index

This function will determine the object type and length and return the appropriate value and its index. If an error occurs on the get, nil is returned.

Example

```
-- Start with port 1
index = “1:1”
-- Get the first link
link = idbU32Get("cpc4400:cpc4400ArchIfaceLink", index)
repeat
    -- Display the last link and index that were gotten
    print(format("Interface %s Link is %d", index, link))
    -- get the next link and its index
    link, index = idbU32GetNext("cpc4400:cpc4400ArchIfaceLink", index)
-- stop when no more links
until (link == nil)
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

This example prints the link interface index and the link status for all links.

Set an Unsigned 32-bit Scalar IDB Object

`idbU32Set(object, index, value)`

Set the IDB object to the value specified.

`object` is a string set to the IDB object name.

`index` is a string set to the MIB table index.

`value` is the value to set the object to. nil is returned on success, else error occurred.

This `idbU32Set` function described above is used to support code supplied in early units, and its use is deprecated. `idbSet()` should be used instead.

Example

```
print (“Drop link on port 7”)
if (idbU32Set("cpc4400:cpc4400ArchIfaceLinkAdmin", "1.7", 2 ) ~= nil)
then
    print (“Error occurred”)
end
```

Set the value of an OBJECT IDENTIFIER type IDB variable

`idbObjIdAnySet(mibObj, index, varbindoid, oid_len, idx_len)`

Used in a Lua script to set the value of an OBJECT IDENTIFIER type IDB variable.

`mibObj` the name of the IDB variable to set

`index` the index of the IDB variable to set.

`varbindoid` the ASN.1 formatted value to set the variable to

`oid_len` not used, set to zero (0)

`idx_len` not used, set to zero (0)

Example

```
-- This example will set the RMON alarm variable for RMON alarm 1 to
-- "cpc4400:cpc4400UsrVarInteger.1". This will allow the value of the
User Defined
-- MIB variable to be reported in the RMON Trap

mibObj = "rfc1757:alarmVariable"
index = "1"
-- this is the ASN.1 ID for the OID "cpc4400:cpc4400UsrVarInteger.1"
varbindoid = "1.3.6.1.4.1.1556.3.6.1.1.2.1"
value = idbObjIdAnySet(mibObj, index, varbindoid, 0, 0)
if value == nil then
    print("PASS")
else
    print("FAIL")
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
end
```

Get an Octet String IDB Object

`idbOctetStringGet(object, index, length)`

Return the value of the IDB object.

`object` is a string set to the IDB object name.

`index` is a string set to the MIB table index.

`length` is the length of the IDB Object. If an error occurs on the get, nil is returned.

Example

```
print(“sysDescr = %s”, idbOctetStringGet("sysDescr", 0, 255))
```

Set an Octet String IDB Object

`idbOctetStringSet(object, index, value)`

Set the value of the IDB object.

`object` is a string set to the IDB object name.

`index` is a string set to the MIB table index.

`value` is the value to set the IDB Object to.

If the set is successful, nil is returned.

Example

```
print(idbOctetStringSet("rfc1213:sysDescr", 0, “cpc4400 Master”))
```

IDB Octet String Object Get Next

`idbOctetStringGetNext (object, index)`

Return the index and the value of the next IDB object in a table of Octet String objects.

`object` is a string set to the IDB object name

`index` is a string set to the MIB table index

This function will determine the object type and length and return the appropriate value and its index. If an error occurs on the get, nil is returned.

Example

The following example prints the IP interface index and name for all interfaces.

```
-- Start with 0
index = 0
repeat
    val, index = idbOctetStringGet-
Next("cpc4400:cpc4400ArchIfaceName",index )
   if ( val ) then
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
            print(format("Interface %s has index %s", val, index))
        end
    until val == nil
```

IDB Helper Functions

The following functions are provided to aid the user in formatting objects or indices when accessing IDB.

IDB Object Formatting Functions

`ip2str (ip)`

Convert a string in dot-separated decimal notation to an octet string. IP Addresses are stored in the MIB as a sequence of octets (an octet string of length 4). For instance, the dotted decimal notation IP Address "147.139.64.1" would be represented in the MIB as a 4 entry array of octets: array[0] = 147, array[1] = 139, array[2] = 64, and array[3] = 1. This function returns the IP Address as an octet string of length 4.

Example

The following example would set the switch gateway address to 147.139.64.100:

```
idbOctetStringSet("cpc4400:cpc4400SwitchIPGateAddress", 0,
            ip2str("147.139.64.100"))
str2ip (idbIP)
```

Convert an IDB formatted IP Address to 4 octets. IP Addresses are stored in the MIB as a sequence of octets (an octet string of length 4). For instance, the dotted decimal notation IP Address "147.139.64.1" would be represented in the MIB as a 4 entry array of octets: array[0] = 147, array[1] = 139, array[2] = 64, and array[3] = 1. This function returns the 4 octets of the string as 4 integers.

The following example would print the dotted decimal version of SIAD.

```
a, b, c, d = str2ip(idbOctetStringGet(
             "cpc4400:cpc4400CommonMiscDHCPClientSIAD", 0, 4))
print(format("SIAD = %d.%d.%d.%d", a, b, c, d))
mac2str (mac)
```

Convert a string in colon separated hexadecimal notation to an octet string. MAC Addresses are stored in the MIB as a sequence of octets (an octet string of length 6). For instance, the colon separated hexadecimal notation MAC Address 00:c0:8c:08:c2:01 would be represented in the MIB as a 6 entry array of octets: array[0] = 0x00, array[1] = 0xc0, array[2] = 0x8c, array[3] = 0x08, array[4] = 0xc1, and array[5] = 0x01. This function returns the MAC Address as an octet string of length 6.

The following example would set the switch gateway address to 147.139.64.100.

```
idbOctetStringSet("rfc2233:ifPhysAddress", 0,
            mac2str("00:c0:8c:08:c2:01"))
str2mac(idbMAC)
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Convert an IDB formatted MAC Address to 6 octets. MAC Addresses are stored in the MIB as a sequence of octets (an octet string of length 6). For instance, the MAC Address 00:c0:8c:08:c2:01 would be represented in the MIB as a 6 entry array of octets: array[0] = 0x00, array[1] = 0xc0, array[2] = 0x8c, array[3] = 0x08, array[4] = 0xc1, and array[5] = 0x01. This function returns the 6 octets of the string as 6 integers.

The following example would print the MAC Address associated with the Switch.

```
a, b, c, d, e, f =str2mac(
     idbOctetStringGet("cpc4400:cpc4400SwitchIPMACAddr", 0, 6))
print(format("MAC Address = %02x:%02x:%02x:%02x:%02x:%02x",
                                          a, b, c, d, e, f))
```

IDB Index Formatting Functions

`nameToOid(string)`

Some of the IDB objects in the MIBs provided with the switch (especially naming objects) use the SnmpAdminString object type as an index. This type is used when an ASCII string name is the index for a table entry. The MIB or IDB OID is a dot-separated decimal representation of the ASCII string that spells the name.

Example

```
index = nameToOid("fred”)
```

The ASCII string “fred” would be converted to an OID value of “102.114.101.100”.

The return string ‘index’ in this example could then be used as a MIB table’s index. This conversion routine can be called to convert the string argument into such an index.

`lnameToOid(string)`

This helper routine is similar to ‘nameToOid’ but the length of the string is also added to the beginning of the returned OID value. This is needed when an Index of type SnmpAdminString does not specify IMPLIED in the INDEX directive.

Example

```
index = lnameToOid("fred”)
```

The ASCII string “fred” would be converted to an OID value of “4.102.114.101.100”.

The return string ‘index’ in this example could then be used as a MIB table’s index. This conversion routine can be called to convert the string argument into such an index.

User-Defined Non-Volatile Variables

The CPC441x provides the user with a number of non-volatile variables that can be set and accessed from SNMP and Lua scripts. There are two classes of variables: integer and string. A table of 5 integer values is available under the variable `cpc4400UsrVarInteger`. A table of 3 string values (with lengths up to 255 characters) is available under the variable `cpc4400UsrVarString`.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

These values are accessed in the same way as any other IDB table variables (`idbU32Get`, `idbU32Set`, `idbOctetStringGet`, etc.). The index values are 1-5 for integers, and 1-3 for strings.

IDB Object Formatting Functions

`ip2str (ip)`

Convert a string in dot separated decimal notation to an octet string. IP Addresses are stored in the MIB as a sequence of octets (an octet string of length 4). For instance, the dotted decimal notation IP Address “147.139.64.1” would be represented in the MIB as a 4 entry array of octets: array[0] = 147, array[1] = 139, array[2] = 64, and array[3] = 1. This function returns the IP Address as an octet string of length 4.

The following example would set the switch gateway address to 147.139.64.100:

```
idbOctetStringSet("cpc4400:cpc4400SwitchIPGateAddress", 0,
            ip2str(“147.139.64.100”))
str2ip (idbIP)
```

Convert an IDB formatted IP Address to 4 octets. IP Addresses are stored in the MIB as a sequence of octets (an octet string of length 4). For instance, the dotted decimal notation IP Address “147.139.64.1” would be represented in the MIB as a 4 entry array of octets: array[0] = 147, array[1] = 139, array[2] = 64, and array[3] = 1. This function returns the 4 octets of the string as 4 integers.

The following example would print the dotted decimal version of SIAD.

```
a, b, c, d = str2ip(idbOctetStringGet(
              "cpc4400:cpc4400CommonMiscDHCPClientSIAD", 0, 4))
print(format("SIAD = %d.%d.%d.%d", a, b, c, d))
mac2str (mac)
```

Convert a string in colon separated hexadecimal notation to an octet string. MAC Addresses are stored in the MIB as a sequence of octets (an octet string of length 6). For instance, the colon separated hexadecimal notation MAC Address 00:c0:8c:08:c2:01 would be represented in the MIB as a 6 entry array of octets: array[0] = 0x00, array[1] = 0xc0, array[2] = 0x8c, array[3] = 0x08, array[4] = 0xc1, and array[5] = 0x01. This function returns the MAC Address as an octet string of length 6.

The following example would set the switch gateway address to 147.139.64.100.

```
idbOctetStringSet("rfc2233:ifPhysAddress", 0,
            mac2str(“00:c0:8c:08:c2:01”))
str2mac(idbMAC)
```

Convert an IDB formatted MAC Address to 6 octets. MAC Addresses are stored in the MIB as a sequence of octets (an octet string of length 6). For instance, the MAC Address 00:c0:8c:08:c2:01 would be represented in the MIB as a 6 entry array of octets: array[0] = 0x00, array[1] = 0xc0, array[2] = 0x8c, array[3] = 0x08, array[4] = 0xc1, and array[5] = 0x01. This function returns the 6 octets of the string as 6 integers.

The following example would print the MAC Address associated with the Switch.

```
a, b, c, d, e, f =str2mac(
     idbOctetStringGet("cpc4400:cpc4400SwitchIPMACAddr", 0, 6))
```


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

```
print(format("MAC Address = %02x:%02x:%02x:%02x:%02x:%02x",
                                              a, b, c, d, e, f))
```

Message Logging

Log a message to the console

`logMsg(message)`

This function logs the message to the console and the log file if logging to a file is enabled.

Example

```
logMsg(“Critical Error occurred”)
```

Test Connectivity to Host

Use ping to test connectivity to a host

`ping(host, count)`

Send ICMP ECHO Request to the host, count time. Return nil if host replies.

Example

```
if (ping (“1.1.1.1”, 1) == nil) then
    print (“1.1.1.1 is alive”)
else
    print (“No response from 1.1.1.1”)
end
```

CLI Commands

Execute a CLI command from Lua

`cli (command)`

Execute the CLI command specified. Command is a string set to the CLI command to execute.

Example

```
cli (“switch display”)
```

Integer Math Functions

The following section describes Performance Technologies additions to the Integer Math Library. The following functions provide bit manipulation capability.

Modulo

`imod(a, b)`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Returns the value of **a** modulus **b** (remainder of **a** divided by **b**).

Bit-wise AND

band(a, b)

Returns the bit-wise 'AND' of **a** and **b**.

Bit-wise OR

bor(a, b)

Returns the bit-wise 'OR' of **a** and **b**.

Bit-wise NOT

bnot(a)

Returns the bit-wise 'NOT' or inversion of **a**.

Bit-wise EXCLUSIVE-OR

bxor(a, b)

Returns the bit-wise 'Exclusive-Or' of a and b.

Bit-wise SHIFT-LEFT

shiftl(a, N)

Returns the result of shifting **a** left N bit positions.

Bit-wise SHIFT-RIGHT

shiftr(a, N)

Returns the result of shifting **a** right N bit positions.

Ejector Handle Status

Get Ejector Handle Status

sysGetEjectorSwitchStatus()

Returns "0" if the ejector handle is locked, "1" if the ejector handle is unlocked, or "-1" if the ejector handle status is not supported.

Note: *Ejector handle status is supported ONLY on the CPC4416. Ejector handle status is NOT supported on the CPC4411. This function ALWAYS returns "-1" on the CPC4411.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

22

Specifications

Overview

This chapter describes the Electrical and Mechanical specifications for the CPC441x.

Electrical

Universal I/O

The CPC441x is a universal I/O board (there is no key on J1), and accepts either 5.0 Vdc or 3.3 Vdc for the PCI I/O signals.

Power Budget

See Table 22-1 and Table 22-2 for a listing of board power consumption.

Table 22-1: CPC4411 Power Consumption

Model and Total Power Consumption	Voltage	Typical Current	Typical Power
CPC4411 29 W max. 22 W typical	3.3 V	3 A	9.9 W
	5 V	3.5 A	17.5 W
	+12 V	0.1 A	1.2 W
	-12 V	0 A	0 W

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 22-2: CPC4416 Power Consumption

Model and Total Power Consumption	Voltage	Typical Current	Typical Power
CPC4416 (without mezzanine card) 25.4 Watts max. 18.5 W typical	3.3 V	1.45 A	4.8 W
	5 V	2.47 A	12.4 W
	+12 V	0.1 A	1.2 W
	-12 V	0.01 A	0.12 W

Voltage Requirements

The following tables show the minimum and maximum voltage requirements.

Table 22-3: CPC4411 Voltage Requirements

Configuration	Voltage	Min	Max
CPC4411	3.3 V	3.14 V	3.47 V
	5 V	4.75 V	5.25 V
	+12 V	10.8 V	13.2V
	-12 V	-13.2V	-10.8 V

Table 22-4: CPC4416 Voltage Requirements

Configuration	Voltage	Min	Max
CPC4416	3.3 V	3.14 V	3.47 V
	5 V	4.75 V	5.25 V
	+12 V	10.8 V	13.2V
	-12 V	-13.2V	-10.8 V

Mechanical

The board adheres to the PICMG 2.0 R3.0 CompactPCI specification. The main board is a 6U CompactPCI board (233.35 mm by 160 mm). The rear panel I/O RTMs (Rear Transition Modules) are 6U boards as well. However, the depth of the RTM board is typically 80 mm.

Operating Temperature: 0□ - 55□ C.

Relative Humidity: 10 - 90% non-condensing.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Battery: The CPC441x includes a surface-mounted lithium battery to maintain the NVRAM across reboots and when the system is turned off. It is unlikely that this battery will need to be replaced during the life of the board. Should replacement be required, reference STMicroelectronics™ part no. M4T28-BR12SH1. It is recommended that a DIP/IC extractor tool be used for removing the battery, rather than a PROM puller.

Caution:
The lithium battery may explode if mishandled. Do not dispose of battery in fire. Do not disassemble battery or attempt to recharge it.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Chapter

23

Rear Transition Modules & Board Pinouts

Overview

This chapter describes the Rear Transition Modules (RTMs) and Pinouts for the CPC441x. The key topics in this chapter include:

- “Rear Transition Modules” on page 492
- “RTM Front Panel Diagrams” on page 494
- “Port Pinouts” on page 496
- “CPC4411 Main Board Pinouts” on page 499
- “FlexLink™ Module” on page 505
- “CPC4416 Main Board Pinouts” on page 505

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Rear Transition Modules

The following Rear Transition Modules are available for use with the CPC4411 and the CPC4416 as shown in Table 23-1: “CPC4411 and CPC4416 RTMs”:

Table 23-1: CPC4411 and CPC4416 RTMs

RTM Assembly	Description	Board	Use
120P1401	5 port	CPC4411F	Fabric
120P2401	2 port	CPC4411F	Fabric
120P0405	24 port single slot	CPC4411E	Enterprise
		CPC4416N	Node
120P0420	24 port dual slot	CPC4411F/CPC4411E	Enterprise
		CPC4416N	Node
120P0401	5 + 2 port	CPC4416F	Fabric
120P0415	24 + 2 port single slot	CPC4416N	Enterprise
120P0425	24 + 2 port dual slot	CPC4416F/CPC4416N	Enterprise

5-Port RTM

The 5-Port RTM is a standard size 6U CompactPCI rear-panel I/O board. It measures 233.35 mm in height and 80 mm in depth as defined by the CompactPCI PICMG 2.0 R3.0 specification. There are no active components on this board. The RTM is connected to the main board through the midplane via the rJ3 and rJ4 CompactPCI connectors. It is used to bring out five 10/100Mb switched Ethernet ports and an RS-232 console port.

2-Port RTM

The 2-Port RTM is a standard size 6U CompactPCI rear-panel I/O board. It measures 233.35 mm in height and 80 mm in depth as defined by the CompactPCI PICMG 2.0 R3.0 specification. There are no active components on this board. The RTM is connected to the main board through the midplane via the rJ3 and rJ4 CompactPCI connectors. It is used to bring out two 10/100Mb switched Ethernet ports and as RS-232 console port.

24-Port Single Slot RTM

The 24-Port Single-Slot RTM is a standard size 6U CompactPCI rear-panel I/O board. It measures 233.35 mm in height and 80 mm in depth as defined by the CompactPCI PICMG 2.0 R3.0 specification. There are no active components on this board. The RTM is connected to the main board through the midplane via the rJ3 and rJ5 CompactPCI connectors. It is used to bring out twenty-four 10/100Mb switched Ethernet ports via two RJ21 Telco connectors. Two 8-foot cables bring these connectors to a 1U-high rack mountable patch panel with 24 RJ45 connectors. The RTM also brings out an RS-232 console port.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

24-Port Dual Slot RTM

The RTM is a standard size 6U CompactPCI rear-panel I/O board. It measures 233.35mm in height and 80mm in depth as defined by the CompactPCI PICMG 2.0 R3.0 specification. It is two card slots wide. There are no active components on this board. The RTM is connected to the main board through the midplane via the rJ3, rJ4, and rJ5 CompactPCI connectors. It is used to bring out 24 10/100Mb switched Ethernet ports and an Out-of-Band Ethernet Management port.

5 + 2 Port RTM

The 5 + 2-Port RTM is a standard size 6U CompactPCI rear-panel I/O board. It measures 233.35 mm in height and 80 mm in depth as defined by the CompactPCI PICMG 2.0 R3.0 specification. There are no active components on this board. The RTM is connected to the main board through the midplane via the rJ3 and rJ4 CompactPCI connectors. It is used to bring out five 10/100Mb switched Ethernet MDIX ports via shielded RJ45 connectors (ports 20-24), two 1000Mb Ethernet MDIX ports (ports 25-26), and an RS232 console port.

24 + 2 Single Slot RTM

The 24-Port Single-Slot RTM is a standard size 6U CompactPCI rear-panel I/O board. It measures 233.35 mm in height and 80 mm in depth as defined by the CompactPCI PICMG 2.0 R3.0 specification. There are no active components on this board. The RTM is connected to the main board through the midplane via the rJ3 and rJ5 CompactPCI connectors. It is used to bring out twenty-four 10/100Mb switched Ethernet ports via two RJ21 Telco connectors. Two 8-foot cables bring these connectors to a 1U-high rack mountable patch panel with 24 RJ45 connectors. The RTM also brings out two 1000Mb Ethernet MDIX ports (ports 25-26).

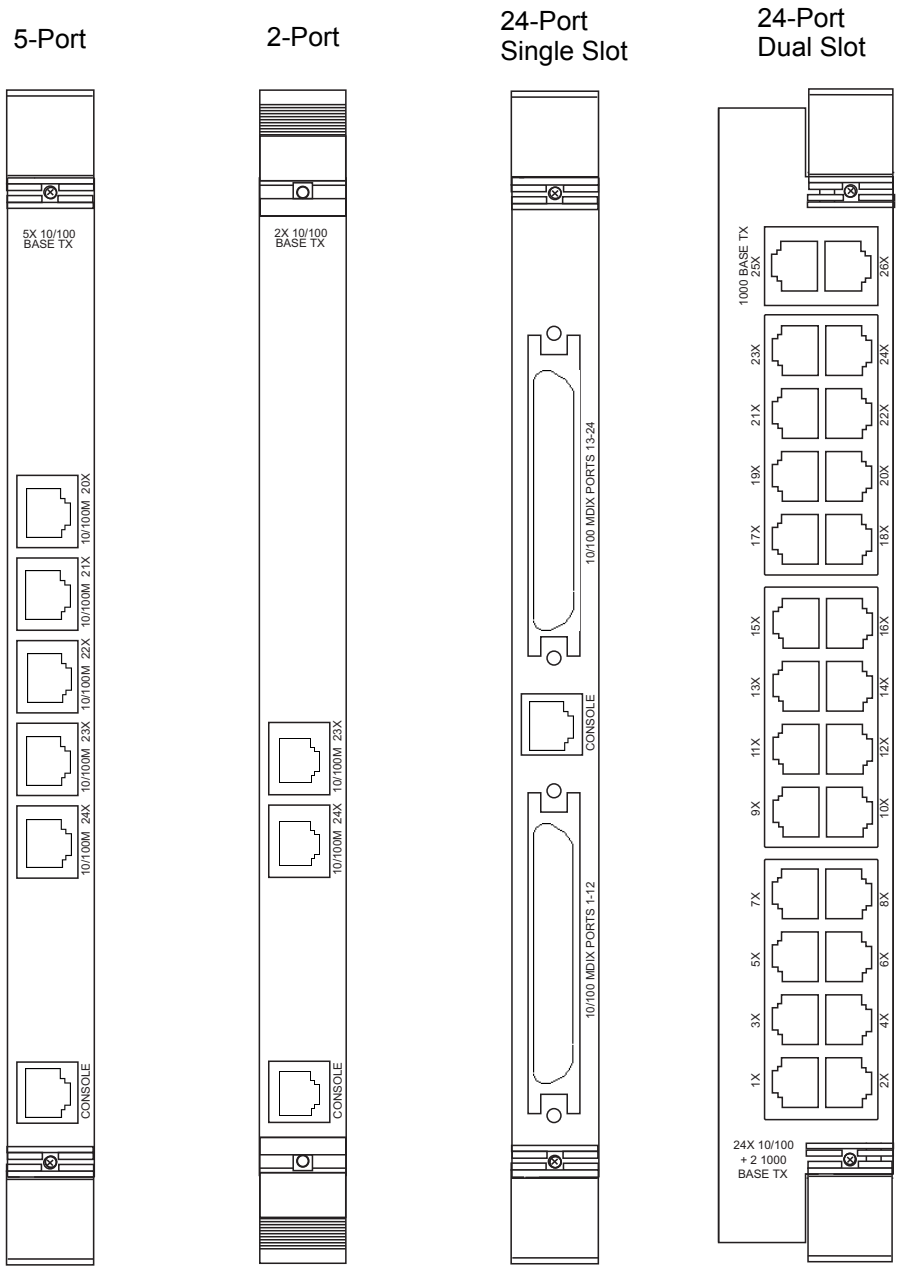
24 + 2 Dual Slot RTM

The 24 + 2-Port RTM is a standard size 6U CompactPCI rear-panel I/O board. It measures 233.35 mm in height and 80 mm in depth as defined by the CompactPCI PICMG 2.0 R3.0 specification. There are no active components on this board. The RTM is connected to the main board through the midplane via the rJ3, rJ4 and rJ5 CompactPCI connectors. It is used to bring out twenty-four 10/100Mb switched Ethernet MDIX ports via shielded RJ45 connectors (ports 1-24), and two 1000Mb Ethernet MDIX ports (ports 25-26).

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

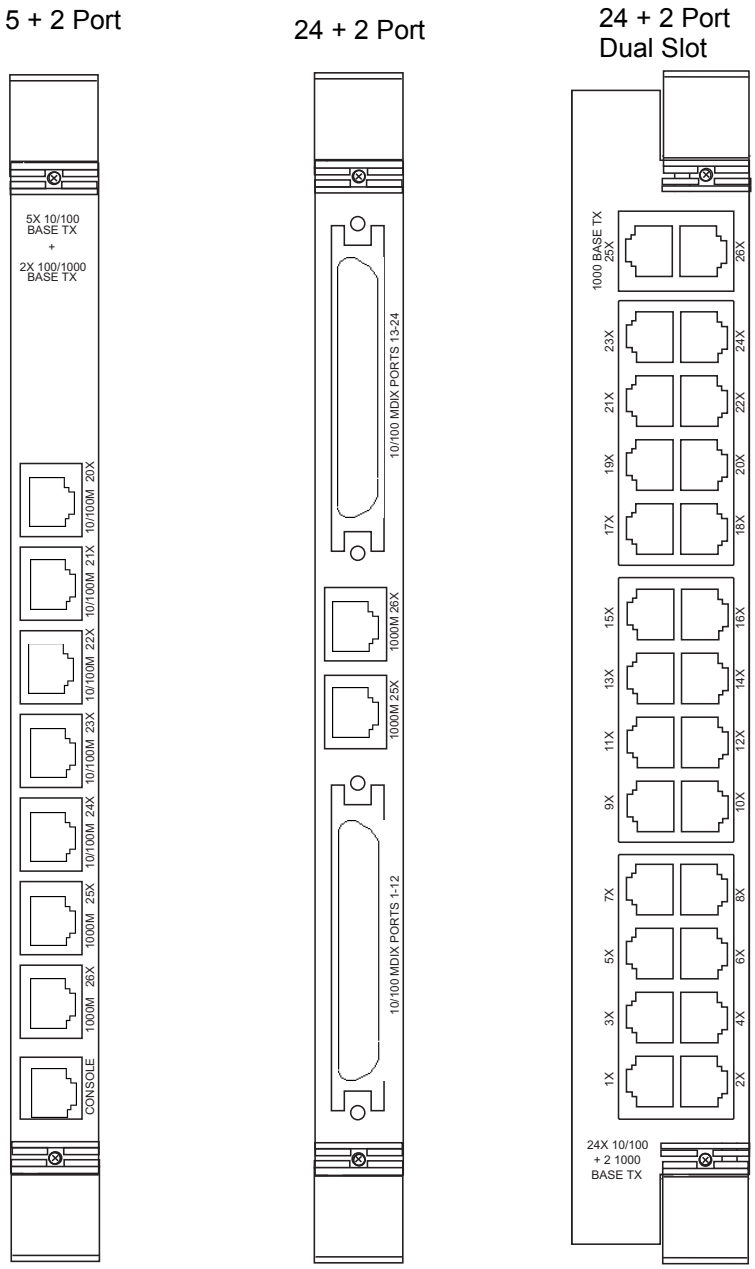
RTM Front Panel Diagrams

Figure 23-1: RTM Front Panel diagrams (1 of 2)



Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Figure 23-2: RTM Front Panel Diagrams (2 of 2)



Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Port Pinouts

10/100Mb Switched Ethernet Ports

The pinout for the switched 10/100Mb Ethernet ports is shown in Table 23-2: “10/100Mb Switched Ethernet Port Pinout”.

Table 23-2: 10/100Mb Switched Ethernet Port Pinout

Pin Number	Signal Name
1	RX+
2	RX-
3	TX+
4	—
5	—
6	TX-
7	—
8	—

1000Mb-Tx Switched Ethernet Ports

The pinout for the switched gigabit Ethernet ports is shown in Table 23-3: “1000Mb Switched Ethernet Port Pinout”.

Table 23-3: 1000Mb Switched Ethernet Port Pinout

Pin Number	Signal Name
1	TRDB+
2	TRDB-
3	TRDA+
4	TRDD+
5	TRDD-
6	TRDA-
7	TRDC+
8	TRDC-

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

1000Mb-Fiber Switched Ethernet Ports

Two Gigabit Fiber ports are supported on the CPC4411. The standard CPC4411 provides for a 1000Base-SX 850nm laser for multi-mode fiber. In addition, a 1000Base-LX 1300nm laser on single or multi-mode fiber can be supported as a custom build. Contact PTI for details. The interface uses the industry standard 1x9 package with SC duplex fiber optic connectors. Transmit and receive differential signals interface to the SERDES at 1.25-GHz. The fiber interface is supported out the front panel of the CPC4411.

Out-of-Band Ethernet Management Port

This port can independently support operation at 10Mb or 100Mb in half-duplex or full-duplex mode. This port is presented to as a standard 100Base-TX MDI connection to a RJ-45 connector on the CPC441x front panel. The pin-out of this port is defined below in Table 23-4: “Ethernet Management Port Pinout”.

Table 23-4: Ethernet Management Port Pinout

Pin Number	Signal Name
1	TX+
2	TX-
3	RX+
4	—
5	—
6	RX-
7	—
8	—

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

RS-232 Console Port

The console port is available on the front panel via a 6-position RJ-11 connector. Several RTMs (through the midplane connection) provide a rear panel 6-position RJ-11 connector for an additional connection point.

Supported signals include TxD and RxD (no support for modem control signals) with RS-232 level signaling. The RJ-11 connector pinout providing a DTE connection is described in Table 23-5: “RJ-11 Console Port Pinout” on page 498.

Table 23-5: RJ-11 Console Port Pinout

RJ-11	I/O	Serial Protocol Name	DUART Connection
1	-	Unused	
2	-	GND	
3	Input	RXD	Receive Data
4	Output	TXD	Transmit Data
5		GND	
6		Unused	

Console Cable

A console cable is available to provide a male DB-9 connector. The cable provides a DTE connection (RS-232 levels), allowing connection to a modem (DCE) without the need of a null modem. A null modem (DB-9F to DB-9F) is provided to allow connection to a terminal or PC (DTE) directly. This cable is 3 feet in length (min). The pinout of the DB-9 is described in Table 23-6: “DB-9 Console Cable Pinout”:

Table 23-6: DB-9 Console Cable Pinout

DB-9	I/O	Serial Protocol Name (EIA574 Mnemonic)	DUART Connection
1	-	Unused	
2	Input	RXD (104)	Receive Data
3	Output	TXD (103)	Transmit Data
4	Output	DTR (108)	NC
5	-	GND (102)	
6	Input	DSR (107)	NC
7	Output	RTS (105)	NC
8	Input	CTS (106)	NC
9	-	Unused	

The male DB-9 connector provides a loopback between DTR and DSR and a loopback between RTS and CTS.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

CPC4411 Main Board Pinouts

The CPC4411 front panel is compliant with the IEEE 1101.10 and IEEE 1101.11 specifications and provides the following functions.

- RJ-11 console port connection. ()
- LEDs for ports and system status.
- Out-of-band Ethernet management port.
- Hard Reset push button.

Port Connections

The CPC4411 provides connectivity of all switched Ethernet ports and the console port to the CompactPCI midplane via J3, J4, and J5. Some ports can be brought out to RJ-45 connectors on a rear panel RTM (Rear Transition Module). The remaining ports are to be connected to other slots in the system via the midplane. The CPC4411 supports twenty-four switched 10Base-T/100Base-TX ports, one out-of-band 10Base-T/100Base-TX port (port 27), and two 1000Base-F ports. Note that (N/E) refers to a Node /Enterprise slot connection and (F) refers to a Fabric slot connection.

Table 23-7: CPC4411 Port Connections

Link Port #	Speed	Connection	Backplane Connector Used
1-8	10/100Base-T	Midplane/Rear Panel I/O	rP3
9-19	10/100Base-T	Midplane/Rear Panel I/O	rP5
20-24	10/100Base-T	Midplane/Rear Panel I/O	rP5(N/E), rP4(F)
25	1000Base-FX	Front Panel I/O	no connection
26	1000Base-FX	Front Panel I/O	no connection
27	10/100Base-T	(Management Port) front panel I/O	--
Console	RS-232C	RJ-11 via RTM or front panel	rP4 (F), rP5 (N/E)

CompactPCI Connectors

The following tables show the pinout information for the CompactPCI midplane connectors.

- Table 23-8: “CPC4411 J1 Connector Pinout” on page 500
- Table 23-9: “CPC4411 J2 Connector Pinout” on page 501
- Table 23-10: “CPC4411 J3 Connector Pinout” on page 502
- Table 23-11: “CPC4411 J4 Connector Pinout (Fabric Only)” on page 503
- Table 23-12: “CPC4411 J5 Connector Pinout” on page 504

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-8: CPC4411 J1 Connector Pinout

Row	A	B	C	D	E	F
25	5V	NC	NC	3.3V	5V	GND
24	NC	5V	V(I/O)	NC	NC	GND
23	3.3V	NC	NC	5V	NC	GND
22	NC	GND	3.3V	NC	NC	GND
21	3.3V	NC	NC	NC	NC	GND
20	NC	GND	V(I/O)	NC	NC	GND
19	3.3V	NC	NC	GND	NC	GND
18	NC	GND	3.3V	NC	NC	GND
17	3.3V	IPMB_SCL	IPMB_SDA	GND	NC	GND
16	NC	GND	V(I/O)	NC	NC	GND
15	3.3V	NC	NC	BD_SEL#	NC	GND
14	KEY					GND
13						GND
12						GND
11	NC	NC	NC	GND	NC	GND
10	NC	GND	3.3V	NC	NC	GND
9	NC	NC	NC	GND	NC	GND
8	NC	GND	V(I/O)	NC	NC	GND
7	NC	NC	NC	GND	NC	GND
6	NC	GND	3.3V	NC	NC	GND
5	NC	NC	RST#	GND	NC	GND
4	IPMB_PWR	HEALTHY#	V(I/O)	NC	NC	GND
3	NC	NC	NC	5V	NC	GND
2	NC	5V	NC	TDO[1]	TDI[1]	GND
1	5V	-12V	NC	+12V	5V	GND

RST#, ENUM#	CompactPCI® PCI Bus related signals (use optional)
HEALTHY#, BDSEL#	CompactPCI® Hardware Connection Control Signals
5V, 3.3V, +12V, -12V	Power pins
IPMB_PWR, _SCL, _SDA	PICMG 2.9 Interface pins (and power)
KEY	IEC 61076-4-101 Key area for PCI I/O signal level (empty)
V(I/O)	I/O Power pins, connect all V(I/O) pins to either 3.3V or 5V
NC	Not Connected

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-9: CPC4411 J2 Connector Pinout

Row	A	B	C	D	E	F
22	GA4[1]	GA3[1]	GA2[1]	GA1[1]	GA0[1]	GND
21	NC	NC	NC	NC	NC	GND
20	NC	NC	NC	NC	NC	GND
19	NC	NC	NC	NC	NC	GND
18	NC	NC	NC	NC	NC	GND
17	NC	NC	NC	NC	NC	GND
16	NC	NC	NC	NC	NC	GND
15	NC	NC	NC	NC	NC	GND
14	NC	NC	NC	NC	NC	GND
13	NC	NC	NC	NC	NC	GND
12	NC	NC	NC	NC	NC	GND
11	NC	NC	NC	NC	NC	GND
10	NC	NC	NC	NC	NC	GND
9	NC	NC	NC	NC	NC	GND
8	NC	NC	NC	NC	NC	GND
7	NC	NC	NC	NC	NC	GND
6	NC	NC	NC	NC	NC	GND
5	NC	NC	NC	NC	NC	GND
4	NC	NC	NC	NC	NC	GND
3	NC	NC	NC	NC	NC	GND
2	NC	NC	NC	NC	NC	GND
1	NC	NC	NC	NC	NC	GND

1. Per PICMG 2.16, CPC4411 provides 0.1uF bypass capacitors to GND on these lines for maximum isolation from J2 non-Ethernet signaling (the 1000Base-T interface has better immunity to its own signaling than to other high edge rate signaling like PCI).

GA[4:0]	Geographic Address per PICMG® 2.16 (isolation row)
NC	Not Connected
GND	Logic Ground

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-10: CPC4411 J3 Connector Pinout

Row	A	B	C	D	E	F
19	SGA4[1]	SGA3[1]	SGA2[1]	SGA1[1]	SGA0[1]	GND
18	NC	NC	GND	NC	NC	GND
17	NC	NC	GND	NC	NC	GND
16	TX8+(F)	TX8-(F)	GND	NC	NC	GND
15	RX8+(F)	RX8-(F)	GND	NC	NC	GND
14	TX7+	TX7-	GND	TX8+(N) or NC (F)	TX8-(N) or NC (F)	GND
13	RX7+	RX7-	GND	RX8+(N) or NC (F)	RX8-(N) or NC (F)	GND
12	TX6+	TX6-	GND	ID3 (N) or NC (F)	ID7 (N) or NC (F)	GND
11	RX6+	RX6-	GND	ID2 (N) or NC (F)	ID6 (N) or NC (F)	GND
10	TX5+	TX5-	GND	ID1 (N) or NC (F)	ID5 (N) or NC (F)	GND
9	RX5+	RX5-	GND	ID0 (N) or NC (F)	ID4 (N) or NC (F)	GND
8	TX4+	TX4-	GND	NC	NC	GND
7	RX4+	RX4-	GND	NC	NC	GND
6	TX3+	TX3-	GND	SERTXD(N) or NC (F)	SERRXD(N) or NC (F)	GND
5	RX3+	RX3-	GND	NC	NC	GND
4	TX2+	TX2-	GND	NC	NC	GND
3	RX2+	RX2-	GND	NC	NC	GND
2	TX1+	TX1-	GND	NC	NC	GND
1	RX1+	RX1-	GND	NC	NC	GND

1. Per PICMG 2.16, CPC4411 will provide 0.1uF bypass capacitors to GND on these lines for maximum isolation from J4 user defined non-Ethernet signaling (the 1000Base-T interface has better immunity to its own signaling than to other high edge rate signaling).

All pins on this connector should be left open on the mid-plane unless specified below.

SGA[4:0]	Shelf Geo. Address per PICMG 2.16 (isolation row)
TRDn	10/100/1000 Link Port
TXn, RXn	10/100 Link Port
ID[7:0]	Reserved for 8-bit rear panel RTM ID
SERTXD, SERRXD	Console (serial) port for RTM
NC	Not Connected

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-11: CPC4411 J4 Connector Pinout (Fabric Only)

Row	A	B	C	D	E	F
25	TX20+ (F)	TX20- (F)	GND	NC	NC	GND
24	RX20+ (F)	RX20- (F)	GND	NC	NC	GND
23	TX21+ (F)	TX21- (F)	GND	NC	NC	GND
22	RX21+ (F)	RX21- (F)	GND	NC	NC	GND
21	TX22+ (F)	TX22- (F)	GND	NC	NC	GND
20	RX22+ (F)	RX22- (F)	GND	NC	NC	GND
19	TX23+ (F)	TX23- (F)	GND	NC	NC	GND
18	RX23+ (F)	RX23- (F)	GND	NC	NC	GND
17	TX24+ (F)	TX24- (F)	GND	NC	NC	GND
16	RX24+ (F)	RX24- (F)	GND	NC	NC	GND
15	NC	NC	GND	NC	NC	GND
14	KEY					GND
13						GND
12						GND
11	NC	NC	GND	NC	NC	GND
10	NC	NC	GND	NC	NC	GND
9	NC	NC	GND	NC	NC	GND
8	NC	NC	GND	NC	NC	GND
7	NC	NC	GND	SERTXD	SERRXD	GND
6	ID3	ID2	GND	ID1	ID0	GND
5	ID7	ID6	GND	ID5	ID4	GND
4	NC	NC	GND	NC	NC	GND
3	NC	NC	GND	NC	NC	GND
2	NC	NC	GND	NC	NC	GND
1	NC	NC	GND	NC	NC	GND

NC	Not Connected
GND	Logic Ground
KEY	PICMG 2.16 Fabric Slot Key
SERTXD, SERRXD	RS-232 Console (Serial) port for rear panel RTM
ID[7:0]	8-bit rear panel RTM Identifier
TRDn	1000 Link Ports
TXn, RXn	10/100 Link Ports

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-12: CPC4411 J5 Connector Pinout

Row	A	B	C	D	E	F
22	TX19+	TX19-	GND	NC	NC	GND
21	RX19+	RX19-	GND	NC	NC	GND
20	TX18+	TX18-	GND	NC	NC	GND
19	RX18+	RX18-	GND	NC	NC	GND
18	TX17+	TX17-	GND	NC	NC	GND
17	RX17+	RX17-	GND	NC	NC	GND
16	TX16+	TX16-	GND	NC	NC	GND
15	RX16+	RX16-	GND	NC	NC	GND
14	TX15+	TX15-	GND	NC	NC	GND
13	RX15+	RX15-	GND	NC	NC	GND
12	TX14+	TX14-	GND	NC	NC	GND
11	RX14+	RX14-	GND	NC	NC	GND
10	TX13+	TX13-	GND	TX20+(N) or NC (F)	TX20-(N) or NC (F)	GND
9	RX13+	RX13-	GND	RX20+(N) or NC (F)	RX20-(N) or NC (F)	GND
8	TX12+	TX12-	GND	TX21+(N) or NC (F)	TX21-(N) or NC (F)	GND
7	RX12+	RX12-	GND	RX21+(N) or NC (F)	RX21-(N) or NC (F)	GND
6	TX11+	TX11-	GND	TX22+(N) or NC (F)	TX22-(N) or NC (F)	GND
5	RX11+	RX11-	GND	RX22+(N) or NC (F)	RX22-(N) or NC (F)	GND
4	TX10+	TX10-	GND	TX23+(N) or NC (F)	TX23-(N) or NC (F)	GND
3	RX10+	RX10-	GND	RX23+(N) or NC (F)	RX23-(N) or NC (F)	GND
2	TX9+	TX9-	GND	TX24+(N) or NC (F)	TX24-(N) or NC (F)	GND
1	RX9+	RX9-	GND	RX24+(N) or NC (F)	RX24-(N) or NC (F)	GND

TRDn	1000 Link Ports
TXn, RXn	10/100 Link Ports
GND	Logic Ground

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

FlexLink™ Module

The CPC4416F/N provides support for one FlexLink™ module. The FlexLink™ site is compatible with PICMG 2.15, PTMC Type 5 specification, also known as PT5MC. FlexLink™ can provide an alternate LAN or WAN interface to the board (such as 1000Base-SX, 1000Base-LX, IP over SONET, ATM over SONET, NAT Server, etc.), or additional processing capability. The CPC4416 provides the 32-bit 33MHz local PCI bus to the FlexLink module.

The module interface also provides support for passing up to two of the switched gigabit and two of the switched 10/100 Ethernet ports to the FlexLink™ module through connections on the user-defined pins of P4. This allows the module to directly interface to the switch fabric at gigabit rates for high-speed packet processing applications.

Several FlexLink™ modules are available from Performance Technologies to take advantage of these port connections, including:

- FlexNAT™ NAT/Load Sharing NAT module
- FlexTunnel™ Secure Access module
- FlexConnect™ module, which brings two 10/100 and two 10/100/1000 TX ports to the front panel.

The PTMC interface supports four Ethernet ports through connections on Jn4, per PICMG 2.15. The mapping is outlined in Table 23-13: “PTMC Port Mapping”.

Table 23-13: PTMC Port Mapping

PTMC Ethernet Port	CPC4416 Port	Port Speed	FlexConnect Port
1	25	10/100/1000Mb	A
2	26	10/100/1000Mb	B
3	23	10/100Mb	C
4	22	10/100Mb	D

CPC4416 Main Board Pinouts

Front Panel

The CPC4416 front panel is compliant with the IEEE 1101.10 and IEEE 1101.11 specifications and provides the following functions.

- RJ-11 console port connection (see Table 23-5: “RJ-11 Console Port Pinout” on page 498)
- LEDs for ports and system status
- Out-of-band Ethernet management port
- Hard Reset push button

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Port Connections

The CPC4416 supports up to twenty-four switched 100Base-T ports, two switched 1000Base-T ports and one out-of-band 100Base-T port (port 27). Only the switched Ethernet ports are connected to the mid-plane. Table 23-14: “CPC4416 Port Connections” details the port connections supported.

Table 23-14: CPC4416 Port Connections

Link Port #	Speed	Connection	Backplane Connector Used
1-8	10/100Base-T	Midplane Rear Panel I/O	rP3
9-19	10/100Base-T	Midplane Rear Panel I/O	rP5
20-21	10/100Base-T	Midplane/Rear Panel I/O	rP5 (Node, Enterprise) rP4(Fabric uplink)[1]
22-23	10/100Base-T	Midplane/Rear Panel I/O /PTMC	rP5(Node, Enterprise) rP4 (Fabric uplink)[1]
24	10/100Base-T	Midplane/Rear Panel I/O	rP3 (F2F Link Port) rP5(Node, Enterprise) rP4 (Fabric uplink)[1,2]
25	10/100/1000Base-T	Midplane/Rear Panel I/O /PTMC	rP3(Node B) rP4 (Fabric uplink)
26	10/100/1000Base-T	Midplane/Rear Panel I/O /PTMC	rP3 (F2F link port) Node A), rP4 (Fabric uplink)
27	10/100Base-T	(Management Port) front panel I/O	--
Console	RS-232C	RJ-11 via RTM and/or front panel	rP4 (Fabric) rP5 (Node, Enterprise)

1. In a PICMG 2.16 Extended Fabric implementation, these ports are normally internal to the midplane; in a Standard Fabric slot, they are uplinks. Any of these ports can be made available as uplink ports via an RTM, provided the midplane does not route Link Port traces to the P4 pins used for that port.
2. Note that the RTM re-directs Link Port 24 to the Fabric-to-Fabric Link Port, not the CPC4416 itself.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

CompactPCI Connectors

The board has standard 2 mm Type A CompactPCI connectors on J1 and J4, and standard Type B connectors on J2, J3, and J5. All switched Ethernet ports, the console port, and all non-switched (out-of-band) management ports are presented to the CompactPCI midplane via connectors J3 and J5. The following tables show the pinout information for the CompactPCI midplane connectors.

- Table 23-15: “CPC4416 J1 Connector Pinout” on page 508
- Table 23-16: “CPC4416 J2 Connector Pinout” on page 509
- Table 23-17: “CPC4416 (Node) J3 Connector Pinout” on page 510
- Table 23-18: “CPC4416 (Fabric) J3 Connector Pinout” on page 511
- Table 23-19: “CPC4416 J4 Connector Pinout - Fabric Only” on page 512
- Table 23-20: “CPC4416 J5 Connector Pinout” on page 514

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-15: CPC4416 J1 Connector Pinout

Row	A	B	C	D	E	F
25	5V	NC	NC	3.3V	5V	GND
24	NC	5V	V(I/O)	NC	NC	GND
23	3.3V	NC	NC	5V	NC	GND
22	NC	GND	3.3V	NC	NC	GND
21	3.3V	NC	NC	NC	NC	GND
20	NC	GND	V(I/O)	NC	NC	GND
19	3.3V	NC	NC	GND	NC	GND
18	NC	GND	3.3V	NC	NC	GND
17	3.3V	IPMB_SCL	IPMB_SDA	GND	NC	GND
16	NC	GND	V(I/O)	NC	NC	GND
15	3.3V	NC	NC	BD_SEL#	NC	GND
14	KEY					GND
13						GND
12						GND
11	NC	NC	NC	GND	NC	GND
10	NC	GND	3.3V	NC	NC	GND
9	NC	NC	NC	GND	NC	GND
8	NC	GND	V(I/O)	NC	NC	GND
7	NC	NC	NC	GND	NC	GND
6	NC	GND	3.3V	NC	NC	GND
5	NC	NC	RST#	GND	NC	GND
4	IPMB_PWR	HEALTHY#	V(I/O)	NC	NC	GND
3	NC	NC	NC	5V	NC	GND
2	NC	5V	NC	TDO[1]	TDI[1]	GND
1	5V	-12V	NC	+12V	5V	GND

1. PICMG 2.0 R3.0 defined JTAG signals (connected via 0 ohm)

RST#	CompactPCI® PCI Bus related signals (use optional)
HEALTHY#, BDSEL#	CompactPCI® Hardware Connection Control Signals
5V, 3.3V, +12V, -12V	Power pins
IPMB_PWR, _SCL, _SDA	PICMG 2.9 Interface pins (and power)
KEY	IEC 61076-4-101 Key area for PCI I/O signal level (empty)
V(I/O)	I/O Power pins, connect all V(I/O) pins to either 3.3V or 5V
NC	Not Connected

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-16: CPC4416 J2 Connector Pinout

Row	A	B	C	D	E	F
22	GA4[1]	GA3[1]	GA2[1]	GA1[1]	GA0[1]	GND
21	NC	NC	NC	NC	NC	GND
20	NC	NC	NC	NC	NC	GND
19	NC	NC	NC	NC	NC	GND
18	NC	NC	NC	NC	NC	GND
17	NC	NC	NC	NC	NC	GND
16	NC	NC	NC	NC	NC	GND
15	NC	NC	NC	NC	NC	GND
14	NC	NC	NC	NC	NC	GND
13	NC	NC	NC	NC	NC	GND
12	NC	NC	NC	NC	NC	GND
11	NC	NC	NC	NC	NC	GND
10	NC	NC	NC	NC	NC	GND
9	NC	NC	NC	NC	NC	GND
8	NC	NC	NC	NC	NC	GND
7	NC	NC	NC	NC	NC	GND
6	NC	NC	NC	NC	NC	GND
5	NC	NC	NC	NC	NC	GND
4	NC	NC	NC	NC	NC	GND
3	NC	NC	NC	NC	NC	GND
2	NC	NC	NC	NC	NC	GND
1	NC	NC	NC	NC	NC	GND

1. Per PICMG 2.16 CPC4416 will provide 0.1uF bypass capacitors to GND on these lines for maximum isolation from J2 non-Ethernet signaling (the 1000Base-T interface has better immunity to its own signaling than to other high edge rate signaling like PCI).

GA[4:0]	Geographic Address per PICMG® 2.16 (isolation row)
NC	Not Connected
GND	Logic Ground

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-17: CPC4416 (Node) J3 Connector Pinout

Row	A	B	C	D	E	F
19	SGA4[1]	SGA3[1]	SGA2[1]	SGA1[1]	SGA0[1]	GND
18	TRD26A+	TRD26A-	GND	TRD26C+	TRD26C-	GND
17	TRD26B+	TRD26B-	GND	TRD26D+	TRD26D-	GND
16	TRD25A+	TRD25A-	GND	TRD25C+	TRD25C-	GND
15	TRD25B+	TRD25B-	GND	TRD25D+	TRD25D-	GND
14	TX7+	TX7-	GND	TX8+	TX8-	GND
13	RX7+	RX7-	GND	RX8+	RX8-	GND
12	TX6+	TX6-	GND	ID3	ID7	GND
11	RX6+	RX6-	GND	ID2	ID6	GND
10	TX5+	TX5-	GND	ID1	ID5	GND
9	RX5+	RX5-	GND	ID0	ID4	GND
8	TX4+	TX4-	GND	NC	NC	GND
7	RX4+	RX4-	GND	NC	NC	GND
6	TX3+	TX3-	GND	SERTXD	SERRXD	GND
5	RX3+	RX3-	GND	NC	NC	GND
4	TX2+	TX2-	GND	NC	NC	GND
3	RX2+	RX2-	GND	NC	NC	GND
2	TX1+	TX1-	GND	NC	NC	GND
1	RX1+	RX1-	GND	NC	NC	GND

1. Per PICMG 2.16, the CPC4416 will provide 0.1uF bypass capacitors to GND on these lines for maximum isolation from J4 user-defined non-Ethernet signaling (the 1000Base-T interface has better immunity to its own signaling than to other high edge rate signaling)
2.For Standard Fabric Slots in PICMG 2.16 (Lilac Blue key in J4), the RTM (per Table 1) supports an option to support Link Port 20 as a Fabric-to-Fabric Link Port on the backplane tails for these pins or No Connects on these pins and Switched Port 20 as Rear I/O. In PICMG 2.16 Extended Fabric Slots (Ocher Yellow key in J4) CPC4416 cannot support a Fabric-to-Fabric Link Port since CPC4416 only has 24 ports maximum and they are all used for Node Slot connectivity.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-18: CPC4416 (Fabric) J3 Connector Pinout

Row	A	B	C	D	E	F
19	SGA4[1]	SGA3[1]	SGA2[1]	SGA1[1]	SGA0[1]	GND
18	NC[2]	NC[2]	GND	NC[2]	NC[2]	GND
17	NC[2]	NC[2]	GND	NC[2]	NC[2]	GND
16	TX8+	TX8-	GND	NC	NC	GND
15	RX8+	RX8-	GND	NC	NC	GND
14	TX7+	TX7-	GND	NC	NC	GND
13	RX7+	RX7-	GND	NC	NC	GND
12	TX6+	TX6-	GND	NC	NC	GND
11	RX6+	RX6-	GND	NC	NC	GND
10	TX5+	TX5-	GND	NC	NC	GND
9	RX5+	RX5-	GND	NC	NC	GND
8	TX4+	TX4-	GND	NC	NC	GND
7	RX4+	RX4-	GND	NC	NC	GND
6	TX3+	TX3-	GND	NC	NC	GND
5	RX3+	RX3-	GND	NC	NC	GND
4	TX2+	TX2-	GND	NC	NC	GND
3	RX2+	RX2-	GND	NC	NC	GND
2	TX1+	TX1-	GND	NC	NC	GND
1	RX1+	RX1-	GND	NC	NC	GND

All pins on this connector should be left open on the midplane, unless specified below.

SGA[4:0]	Shelf Geographic Address per PICMG 2.16 (isolation row)
TRDn	10/100/1000 Link Port
TXn, RXn	10/100 Link Port
ID[7:0]	Reserved for 8-bit rear panel RTM ID
SERTXD, SERRXD	Console (serial) port for RTM
NC	Not Connected

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-19: CPC4416 J4 Connector Pinout - Fabric Only

Row	A	B	C	D	E	F
25	TX20+[1]	TX20-[1]	GND	NC	NC	GND
24	RX20+[1]	RX20-[1]	GND	NC	NC	GND
23	TX21+	TX21-	GND	NC	NC	GND
22	RX21+	RX21-	GND	NC	NC	GND
21	TX22+	TX22-	GND	NC	NC	GND
20	RX22+	RX22-	GND	NC	NC	GND
19	TX23+	TX23-	GND	NC	NC	GND
18	RX23+	RX23-	GND	NC	NC	GND
17	TX24+	TX24-	GND	NC	NC	GND
16	RX24+	RX24-	GND	NC	NC	GND
15	NC	NC	GND	NC	NC	GND
14	KEY					GND
13						GND
12						GND
11	NC	NC	GND	NC	NC	GND
10	NC	NC	GND	NC	NC	GND
9	NC	NC	GND	NC	NC	GND
8	NC	NC	GND	NC	NC	GND
7	NC	NC	GND	SERTXD	SERRXD	GND
6	ID3	ID2	GND	ID1	ID0	GND
5	ID7	ID6	GND	ID5	ID4	GND
4	TRD26A+(F) or NC(F2F)	TRD26A-(F) or NC(F2F)	GND	TRD26C+(F) or NC(F2F)	TRD26C-(F) or NC(F2F)	GND
3	TRD26B+(F) or NC(F2F)	TRD26B-(F) or NC(F2F)	GND	TRD26D+(F) or NC(F2F)	TRD26D-(F) or NC(F2F)	GND
2	TRD25A+	TRD25A-	GND	TRD25C+	TRD25C-	GND
1	TRD25B+	TRD25B-	GND	TRD25D+	TRD25D-	GND

1. For PICMG 2.16 Standard Fabric Slots, the RTM supports an option for connecting Link Port 20 to the F2F Link Port via the backplane tails on rP3 rows 17 and 18. For PICMG 2.16 Extended Fabric, support of the F2F Link Port is not possible since CPC4416 has only a maximum of 24 ports, which are all used to connect to the 24 Node Slots.

NC	Not Connected
GND	Logic Ground
KEY	PICMG 2.16 Fabric Slot Key

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

SERTXD, SERRXD	RS-232 Console (Serial) port for rear panel RTM
ID[7:0]	8-bit rear panel RTM Identifier
MGMT_Tx/Rx	Management Port midplane connections
TRDn	10/100/1000 Link Ports
TXn, RXn	10/100 Link Ports

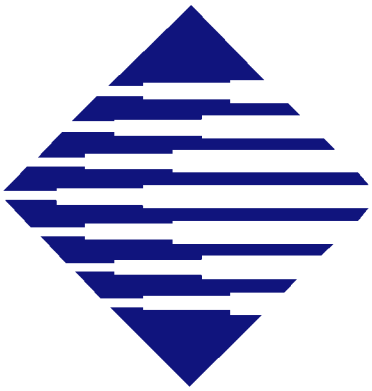
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Table 23-20: CPC4416 J5 Connector Pinout

Row	A	B	C	D	E	F
22	TX19+	TX19-	GND	NC	NC	GND
21	RX19+	RX19-	GND	NC	NC	GND
20	TX18+	TX18-	GND	NC	NC	GND
19	RX18+	RX18-	GND	NC	NC	GND
18	TX17+	TX17-	GND	NC	NC	GND
17	RX17+	RX17-	GND	NC	NC	GND
16	TX16+	TX16-	GND	NC	NC	GND
15	RX16+	RX16-	GND	NC	NC	GND
14	TX15+	TX15-	GND	NC	NC	GND
13	RX15+	RX15-	GND	NC	NC	GND
12	TX14+	TX14-	GND	NC	NC	GND
11	RX14+	RX14-	GND	NC	NC	GND
10	TX13+	TX13-	GND	TX20+(N) or NC (F)	TX20-(N) or NC (F)	GND
9	RX13+	RX13-	GND	RX20+(N) or NC (F)	RX20-(N) or NC (F)	GND
8	TX12+	TX12-	GND	TX21+(N) or NC (F)	TX21-(N) or NC (F)	GND
7	RX12+	RX12-	GND	RX21+(N) or NC (F)	RX21-(N) or NC (F)	GND
6	TX11+	TX11-	GND	TX22+(N) or NC (F)	TX22-(N) or NC (F)	GND
5	RX11+	RX11-	GND	RX22+(N) or NC (F)	RX22-(N) or NC (F)	GND
4	TX10+	TX10-	GND	TX23+(N) or NC (F)	TX23-(N) or NC (F)	GND
3	RX10+	RX10-	GND	RX23+(N) or NC (F)	RX23-(N) or NC (F)	GND
2	TX9+	TX9-	GND	TX24+(N) or NC (F)	TX24-(N) or NC (F)	GND
1	RX9+	RX9-	GND	RX24+(N) or NC (F)	RX24-(N) or NC (F)	GND

TRDn	10/100/1000 Link Ports
TXn, RXn	10/100 Link Ports
GND	Logic Ground

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com



Index

A

admitall
  set on a set of ports 126

ARP table
  add entry 136
  display 135
  flush entries 137
  remove entry 136

ARP verify, configure 136

auto MDX 301

auto polarity sense 301

autonegotiation 302
  configure advertisement parameters 182
  restart 184

autonomous system border router, set 190

B

beacon
  configuration examples 81
  create 79
  destroy 80
  display 80

board-level system status LEDs 68

boot process 63

boot.lua 63, 428

BootP client
  configure 83
  display all configured 84
  display or set interface name 82
  display or set VLAN ID 82
  enable or disable 82
  remove 83
  set timeout value 83

boot-time tests 63

border gateway filtering, enable or disable 188

BPDU filters, enable or disable 113

broadcast storm 34

C

CLI
  beacon configuration commands 79
  BootP commands 82
  class of service (CoS) commands 85
  command history commands 128
  command summary 78
  console port commands 88
  control key commands 76
  date and time commands 90
  DHCP client/server commands 91
  escape key commands 77
  event manager commands 96
  exit 209
  file system commands 100
  file transfer commands 106
  filter mask commands 110
  filtering database commands 115
  GARP commands 120
  GVRP commands 125
  IGMP snooping commands 129
  internet protocol (IP) commands 132
  IPMI FRU commands 138
  IPMI PM commands 149
  link aggregation commands 152
  log commands 172
  network diagnostics commands 175
  online integrity test configuration 178
  OSPF commands 189
  password commands 180
  port commands 181
  RIP commands 186
  routing commands 186
  shell commands 208
  SNMP commands 211
  spanning tree commands 225
  switch management commands 237
  switch security commands 241
  threshold commands 247
  typographic conventions 73

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

user name commands 249
VLAN commands 250
VRRP commands 254

command history, display 128

command line help, display 209

configuration, capture current into CLI script 105

console display height, set 88

console display width, set 89

console port 62, 498

console port baud rate, set 88

conventions 4

COS 35
display current queue configuration 85
display or set default for port 85
processing, enable/disable 85
set queuing algorithm to strict 86
set queuing algorithm to weighted round robin 86

CPU mirror mode, enable or disable 175

current working directory, display 102

customer support and services 26

D

date and time, display or set 90

default
password 64
route redistribution, enable or disable 198
route, advertise 187
settings, restoring 443
TTL, configure 135

de-register script when event is detected 98

DHCP
BootP client 422
configuration file 414
lease section 416
port client ID 420
relay agent example 421
sample dhcps.conf file 421
server configuration 414
vendor options 422

DHCP client
configure 93
display all configured 94
display or set ID 92
display or set retry count 92
display or set VLAN ID 92
enable or disable 91
remove 93
set listen port 91
set transmit port 91

DHCP server
enable/disable 94
set configuration file 94
set logging level 95

dhcps.conf 427

diagnostic tools 36, 445
ping 446
port mirrors 445
traceroute 446

directory hierarchy
change positions 102
create new within hierarchy 101

durable file 427

E

echo a message 208

egress ports, set to be mirrored 176

ejector handle status 485

electrostatic discharge, warning 4

event
addd 97
list currently registered through CLI 99
names and descriptions 96
remove 98

execution, suspend 208

exit 64

F

fabric board 30

fabric-to-fabric link options 54

fast port 34, 230

fast uplink 33, 369

fault LED 69

fault state 448

FCC (USA) Class A notice 3

FDB, see filtering database 309

file
check for existence 105
compare 104
copy 103
display contents 105
edit 103
remove 102
rename 103

file system 425
board application software recovery 432
boot.lua 428
booting from a TFTP server 435, 436
booting from another switch 440
booting with an alternate image 434
chek for errors 101
configuring switch software 440
dhcps.conf 427
durable file 427
list file in 100
log.msg 427
mount 100
persist file 427

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

rc.lua 428
remote file systems 426
restoring factory defaults 443

filter mask
add 110
delete 111
display non-system table 110

filter rule
add 112
delete specified 114

filter rule table,display non-system 111

filtering database 309
add static multicast entry 116
add static unicast entry 118
delete entries from permanent multicast 117
delete entries from unicast 119
delete permanent multicast 117
display 115
display or set aging time 115
display unicast 118
flush 115

flash
/postlogin_banner 428
/prelogin_banner 428

forward all
display or set multicast port list 123
display or set port list 123

forward unregistered
display or set multicast port list 123
display or set port list for which GMRP forbidden 124

forwarding, configure 135

FRU board area
display length value 139
display or set custom manufacturing area 1 value 142
display or set custom manufacturing area 2 value 142
display or set custom manufacturing area 3 value 143
display or set file ID value 141
display or set format version value 139
display or set lanaguage code value 140
display or set manufacturer name namue 140
display or set manufacturing date value 140
display or set part number value 141
display or set product name value 141
display or set serial number value 141

FRU board information, display 143

FRU common header information, display 139

FRU product area
display information 148
display length value 144
display or set asset tag value 146
display or set custom product info 1 value 147
display or set custom product info 2 value 147
display or set custom product info 3 value 148
display or set file ID value 147
display or set format version value 144
display or set language code value 144
display or set manufaturer name value 145
display or set product name value 145
display or set product version value 146
display or set serial number value 146
display orr set model number value 145
set values in 148

FRU, display information 138

FTP 36
display or set server logging level 108
set password 107
use to transfer files 106

FTPD
set user name 107

G

GARP 120
set join time 120
set leave time 120
set leaveall time 120

gateway, assign default 133

GMRP 35
display or set port list 123
display status 122
enable/disable 122
enable/disable on set of ports 122

GVRP 125
configure port priority 125
display status on a list of ports 127
enable/disable 125
enable/disable on a set of ports 125

H

hotswap.lua 451

HTTP-based management 297

I

IGMP snooping
disable 129
display or set age timer 130
display or set query expiry time on a VLAN 131
display or set query interval on a VLAN 131
enable 129
enable or disable 129
enable query agent on VLAN 130
show current memberships 130
show current query status 131

ingress ports, set tp be mirrored 176

initialization tests 63

installation 61

integer MIB object, display or set 210

integrated access device (IAD) 40

integrated server farm 41

interface
delete 134
remove from OSPF 194
specify to be advertised and associate with an area 194

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

IP address associated with interface, delete 134
IP DSLAM device 40
IP interface, configure 132
IPMI transaction statistics information, display 151

L

layer 4-7 packet filtering 311
learning, set up managed for port 119
LEDs
  board-level system status LEDs 68
  fault 69
  hot swap 69
  port 68
  system 68
link aggregation 385
  administrative keys 386
  and spanning tree 392
  architecture overview 388
  assign actor key value 164
  assign actor system priority value 163
  assign distribution criteria 162
  assign partner key value 167
  assign partner port value 167
  assign partner state 168
  configuration examples 394
  configure partner ID 166
  configure static no timeout 169
  default settings 386
  display aggregator configuration 154
  display churn detection state machine information 170
  display D 152
  display LAC aggregator port information 156
  display LAC port information 155
  display or set link decision method 168
  display or set states 165
  display states 153
  display statistics 159
  display timers 157
  distribution rules (rtag) 387
  enable or disable 152
  LACPDU transmission interval (timeout) 388
  set maximum delay 164
  set port priority 165
  set ports as aggregatable 163
  set timeout 166
  state machines 400
  switch configurations 395
link state database, display 200
log.msg 427
logging
  enable or disable console 172
  enable or disable remote 173
  enable or disable to a file 172
  in 64
  set IP address of remote 173
  set the log file name 173
  write a message 172
logical link control (LLC) 32
login, FTP 107
logout 64
LSAs, disabling opaque 341
Lua programming language 449
  hotswap.lua 451
  re.lua 450
  recovercfg.lua 461
  savecfg.lua 459

M

MAC address, determining 61
mapping, set for priority to queue 86
message of the day 428
MIBs 262, 263
mirror mode, set 175
mirror to port, set 176
mirroring 34, 175
mount point, remove 101

N

network services 36
network statistics, display 133
node board 30

O

octet string MIB object, display or set 209
online integrity test 446
  display or set and action for 179
  display or set level one timer value 179
  display the current settings 179
  enable, disable or display all level two 178
  enable, disable, display all level one 178
  enable, disable, or display 178
  level one 447
  level two 447
opaque LSAs, enable or disable 190
OSPF 337
  adjacency 339
  advertise routes 188
  areas 341
  authentication 352
  configure interface 193
  designated router and backup designated router 339
  display area 193
  display general settings 199
  display interface table 197
  display neighbors 201
  enable or disable 189
  link state advertisements (LSAs) 340
  multiple area configuration example 347
  neighbor table 339
  remove area 193

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

routing table 339
set authentication key 195
set authentication type 195
set dead interval 195
set hello interval 196
set interface priority 197
set transit delay 196
single area configuration example 342
timers 352
topology table 338
virtual link 352

out-of-band (management) Ethernet port 33

P

packet filtering
action bits 314
examples 316
mask table 313
matching 315
multiple actions and conflict resolution 315
packet key 317
rules 314

packet switching backplane 30

password
FTPD 107
initial setting 64

path cost 229

PCI signals 32

persist 427

ping 177, 446

pinouts 491
out-of-band management port 497
switched Ethernet port 496

PM controller
display firmware version 150
display geographic address seen by 149
display GUID value of 149
display information 150
reprogram firmware 150
reset 149
reset IPMI transaction statistics 150

POC 63

port
configuration 301
configure 181
configure frame size 184
display statistics for 184
give a symbolic name to 181
set a link for 182

port LEDs 68

port mirror 445

power-on confidence (POC) tests 63, 446
enable or disable 239

product warranty 27

programming interface 37

public key
add client to registry 245
display client stored in registry 246
export host to ASCII format 245
generate new host and private keys 245
remove a client from registry 246

PVID, associate with a set of ports 127

Q

quality of service 35

R

rc.lua 64, 428, 450

recovercfg.lua 461

register script to invoke upon detection of event 97

return merchandise authorization (RMA) 26

RFC
1213 262
1493 262
1757 262
2132 420
2674 262

RIP 334
disable on a particular interface 189
display configuration 189
enable or disable 186
packet formats 335
route redistribution, enable or disable 199
set configuration 186
statistics, display per port 188
timers 335

RIP 2 334

router ID, set 190

routing protocols 325

routing table, display complete 207

RS-232 port 498

S

savecfg.lua 459

script file, execute 208

secure host IP
add entry 241
delete entries from database 242
display database 242

serial port 498

SNMP 261
MIBs 262
trap configuration 263

SNMP community
display entry 219
remove 218
set name and permissions 218

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

SNMP notify filter table
configure entry . . . 211
delete entry . . . 211
display . . . 212

SNMP notify profile table
delete entry . . . 212
display . . . 213
set up . . . 213

SNMP notify table
configure entry . . . 214
delete entry . . . 213
display entries . . . 214

SNMP target address table
configure entry . . . 215
delete entry . . . 215
display entries . . . 216

SNMP target parameters table
delete entry . . . 216
display . . . 218
set entry . . . 217

SNMP3
add access . . . 222
add group . . . 223
add user . . . 219
add view entry . . . 221
configure security . . . 244
delete access . . . 222
delete group . . . 223
delete user . . . 220
delete view . . . 221
display users . . . 220
show access . . . 223
show group . . . 224
show views . . . 221

SNMPV1/V2c security, configure . . . 243

spanning tree
and link aggregation . . . 392
associate enable with VLAN creation . . . 234
backup root port . . . 372
designate port as edge port (RSTP) . . . 235
display or set bridge priority . . . 227
display or set forward delay time . . . 228
display or set hello time . . . 227
display or set max age time . . . 228
display or set port priority . . . 234
display status . . . 229
enable or disable . . . 227, 232
enable or disable a port . . . 233
enable or disable fast port on port . . . 233
enable or disable fast uplink . . . 228
enable or disable port . . . 233
enable or disable protocol on port . . . 232
fast port . . . 230
fast uplink . . . 369
fast uplink group . . . 371
force port to transmit an RSTP BPDU . . . 235
path cost . . . 229
priority . . . 230
select admin point-to-point on port (RSTP) . . . 234
select RSTP compatibility version (RSTP) . . . 236
set path cost style . . . 226
set transmit hold count (RSTP) . . . 236
set version . . . 225
states . . . 369
VRRP . . . 362

specifications
battery . . . 489
electrical . . . 487
IEEE 802.1Q . . . 35, 303, 312
IEEE 802.1q . . . 262
IEEE 802.3 . . . 33, 302
IEEE 802.3ad . . . 62
IEEE802.3ad . . . 400
mechanical . . . 488
PICMG 2.16 . . . 30

SSH
configure port listening . . . 244
enable or disable . . . 244

static route
add . . . 206
advertise . . . 187
delete . . . 206
display . . . 207
enable or disable redistribution . . . 199

stub area
add new . . . 192
display all . . . 192
remove . . . 191
set and metric . . . 191

switch
display information . . . 237
reset . . . 237
reset to factory default values . . . 237
save configuration . . . 104

syslogd . . . 173, 174

system files, update . . . 238

system LED . . . 68

system password, set . . . 180

T

telnet security, configure . . . 243

TFTP . . . 36
set server logging level . . . 109
use to transfer files . . . 106

TFTPD
display or set maximum concurrent connections . . . 109
display or set time to wait between retries . . . 108
display or set timeout for transfers . . . 108
set write access . . . 107

threshold
enable or diasable multicast . . . 247
enable or disable broadcast . . . 247
enable or disable flood . . . 248
set rate control . . . 247

time set for remote NTP server . . . 90

traceroute . . . 177, 446

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

trunk group, display information 160
trunk group, display mapping 161

U

user name
FTPD 107
modify 249

V

version information, display 240

virtual connection
create 202
display 206
remove 204
set authentication key 202
set authentication type 203
set dead interval 203
set hello interval 205
set retransmit interval 205
set transit delay 204

VLAN 303
add ports 252
configuration 305
configuring for VRRP 360
create 250
destroy 251
destroy all 251
display or set name 251
display status summary 250
port parameters 305
remove ports 252
set ingress filter mode 126
show status 253
static VLANs 305

VRRP 357
backup router 358
configuration examples 362
configuring GVRP 361
configuring simple VRRP interface router 360
configuring VLANs 360
delete instance 255
display information 258
display or set advertisement interval 257
display or set authentication mode 256
display or set authentication password 257
display or set enable 255
display or set master down interval count 260
Display or set preempt mode 256
display or set priority 255
display statistics 258
enable or disable fast feature 258
master router 358
set interface to participate in 254
spanning tree 362
virtual interface router 358
virtual router identifier 358
VRRP router 358

W

warranty, product 27
watchdog timer, enable or disable reboot 238
watchdog, enable or disable 237
web management 297
enable or disable 240

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP