Release Notes for Cisco Enhanced Device Interface 2.0

September 23, 2007

These release notes support the release of Cisco Enhanced Device Interface 2.0.

Contents

This document includes the following topics:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2003 - 2005 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco E-DI 2.0 is a new release of Cisco E-DI.

Cisco E-DI provides a comprehensive management interface for configuration of Cisco devices. Cisco E-DI offers interfaces for two categories of users - the human user interacting with network devices through the command line interface (CLI), and management applications interacting with network devices through an XML programmatic interface (see *Cisco Enhanced Device Interface Programmer's Guide, 2.0)*.

Installation

Refer to the *Cisco E-DI Quick Start Guide 2.0* for details to install, configure and start using Cisco E-DI.

Incremental Device Updates

IDUs allow Cisco E-DI to be updated with support for new device packages.

The device packages listed in Table 2 are included in this build.

The device packages listed in Table 3 are available through CCO. To add these packages, the Cisco E-DI administrator can login to CCO, specify the Cisco E-DI version, and download the files for the device packages. See http://www.cisco.com/kobayashi/sw-center/sw-netmgmt.shtml. Once the required device package files are downloaded, they can be copied to Cisco E-DI, and installed using the maintenance shell. Refer to *Cisco E-DI Quick Start Guide 2.0* for details of the installation process.

Important Notes

Forbidden Commands

Administrator can restrict certain native device commands that can be executed on the device using the **exec-cmd** command. These commands can be added to /user/admin/forbiddenCommands file. Each command must be entered on a separate line. Users will not be allowed to execute any command that matches or starts with the commands entered in the file. Use **edit** command to edit this file. Only the Administrator is allowed to edit. The default content of forbiddenCommands file is as follows: **er** <cr> **erase** <cr> **wr** <cr> **write** <cr> **re** <cr> **reload**.

Known Caveats With This Release

Open Caveats

Table 1 Open Caveats

Identifier	Title	Impact	Workaround
CSCeh59930	The editor process (opened using the edit command) or the perl process are not closed when the user session times out.	This might effect the performance of Cisco E-DI if too many sessions are opened.	None.
CSCeh67305	Startup config is retrieved even though it has been erased on device. The configuration is retrieved from the archives on Cisco E-DI.	None.	None.

Table 1 Open Caveats (continued)

Identifier	Title	Impact	Workaround
CSCjh00074	The security check for file and directory operations using perl commands fails.	A Cisco E-DI perl script user with less privileges can perform operations that the user is not authorized to.	Limit the usage of perl scripts for manipulating the Cisco E-DI file system.
CSCeh94947	The device status shows offline when SNMP connectivity fails but Telnet connectivity exists.	Device status is misleading.	Check SNMP credentials on Cisco E-DI configuration and on the NE.
CSCeh73442	The utility command **snmp oidlookup** fails with an **internal error** message.	None.	Cisco MIB lookups can be performed online at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.
CSCeh77656	In group config mode, interface selection behavior is inconsistent.	Interface selection is not allowed in group config mode, except in the interface configuration.	Do the same operation on individual devices.
CSCei09354	A user with netoperator privileges cannot view locks acquired.	The user will be unable to see the locks acquired on the devices in their domain.	Try acquiring the lock on the desired device. If another user has acquired a lock already, the operation will fail indicating the owner.
CSCei10176	**http-raw-request** command is handled incorrectly on XML PI.	Inconsistencies in XML PI behavior will be seen when **http-raw-request** submode is part of the configuration of a device.	None.

Table 1 Open Caveats (continued)

Identifier	Title	Impact	Workaround
CSCin88776	Unable to close editor in Telnet and SSH.	The editor cannot be closed in Telnet or SSH sessions when opened through certain clients like MS-DOS.	Use applications such as Putty.
CSCin93495	Cisco E-DI does not support concurrent connections beyond 64.	A user cannot open more than 64 concurrent sessions on Cisco E-DI.	None.
CSCjh00139	In connect exec mode the write commands do not ask for confirmation.	It is possible to inadvertently perform destructive operations through connect exec mode.	Exercise caution when using the connect exec mode.
CSCei17032	Download of files from ftp-server works only for anonymous users.	Download operation fails if **anonymous** user access is disabled on FTP server.	Use **download http://url** or **copy tftp://TFTPServer** commands to download files from external servers
CSCin93297	The derived credential set will inherit the credentials from a parent set when it is re-created after deletion.	Inconsistencies in the state of devices may be seen.	Do not create a credential set with different credentials than the original parent set, and the same name.

Known Limitations with IDUs

Cisco IOS Devices

The following are known limitations with the Incremental Device Updates (IDUs) for the Cisco IOS devices listed in Table 2 and Table 3:

1. Implicit support provides a super-set/sub-set CLI of what is supported on a particular device type.

2. The following commands are not supported in network config mode:
   a. do
   b. define
   c. interface range
   d. default
   e. help
3. Only the following commands are supported in network exec mode:
   a. clear
   b. clock
   c. erase
   d. show
   e. write
4. Complete syntax checking for some commands in the following scenarios may be not be available:
   a. access-list (syntax checks available to depth 7)
   b. redistribute (syntax checks available to depth 5)—The user will see a customized node WORD with description Command Parameters. This node will accept any syntax, and will recurse to an infinite depth.
5. Some commands may not have a <cr>. This can occur for deprecated commands or any Cisco IOS commands that need special handling.
6. Hidden commands supported by Cisco IOS will not be supported through Cisco E-DI.

CatOS Devices

The following are known limitations with the Incremental Device Updates (IDUs) for the Cisco CatOS devices listed in Table 2 and Table 3:

1. Implicit support provides a super-set/sub-set CLI of what is supported on a particular device type.

2. Only the following commands are supported in network config mode:
   a. set
   b. clear
   c. commit
3. Only the following commands are supported in network exec mode:
   a. show
   b. history
   c. disconnect
   d. reconfirm
   e. reset
   f. slip
   g. switch
   h. rollback
4. Complete syntax checking for some commands in the following scenarios may not be available:
   a. set vlan <vlan> name
   b. set security acl—The user will see a customized node WORD with description Command Parameters. This node will accept any syntax and will recurse to an infinite depth.
5. Some commands may not have a <cr>. This can occur for deprecated commands or any CatOS commands that need special handling.
6. Hidden commands supported by CatOS will not be supported through Cisco E-DI.
7. Interactive commands that require user input after a carriage-return is typed will not be not supported. For example :
   - issc-6509-2> (enable) set password
   - issc-6509-2> (enable) set enablepass

Devices Supported by Cisco E-DI

The device packages listed in Table 2 are included in this build.

The device packages listed in Table 3 are available through CCO. See http://www.cisco.com/kobayashi/sw-center/sw-netmgmt.shtml.

Note When additional device packages are supported, they will be made available through CCO.

Table 2 IDUs Available on Cisco E-DI Product CD-ROM

IDU	OS Version	IDU Version
Cisco12000	12.0(27)S5	1.1
Cisco7600	12.2(18)SXD4	1.1
Cat6500	12.1(11b)E1, 12.2(17d)SXB6	1.2
Cisco1700	12.2(15)T14, 12.3(8)T6	1.2
Cat6500CatOS	7.6(6)	1.1
Cat3550	12.1(14)EA1a, 12.1(22)EA2	1.2
Cat4000	12.1(19)EW1	1.1
Cisco7200	12.2(13)T14	1.1
Cat2950	12.1(13)EA1c	1.1
Cisco2600	12.1(17), 12.2(24a)	1.2

Table 3 IDUs Available on CCO

IDU	OS Version	IDU Version
Cisco800	12.3(8)T7	1.1
CiscoAP350IOS	12.3(2)JA2	1.1
Cat3750	12.1(19)EA1a	1.1

Devices Not Supported by Cisco E-DI

The list of unsupported devices can be seen using the command **show devices**. An asterisk (*) indicates that a device is not supported, and an IDU is not available.

Related Documentation

Refer to the following publications for additional information:

- *Cisco Enhanced Device Interface Quick Start Guide, 2.0*
- *Cisco Enhanced Device Interface User's Guide, 2.0*
- *Cisco Enhanced Device Interface Programmer's Guide, 2.0*
- *Cisco IDU Read-me Files*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)