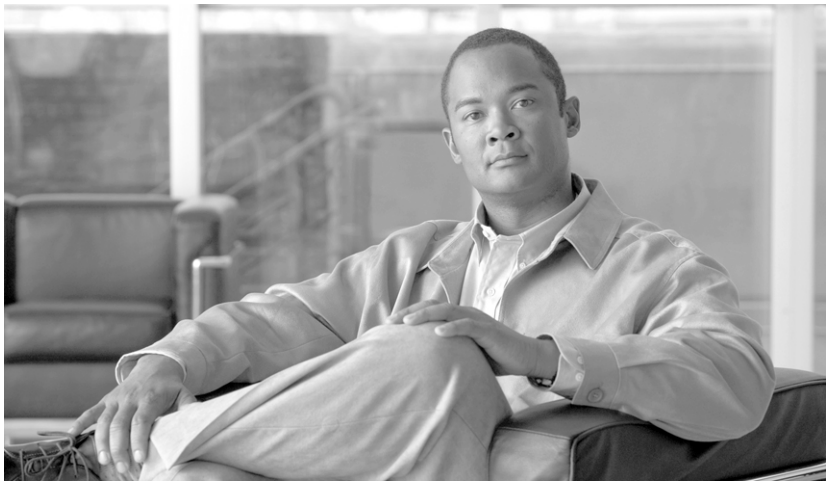


# User Guide for Cisco Enhanced Device Interface

Software Release 2.2

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12567-01

# CONTENTS

# Preface

This guide explains how to use Cisco Enhanced Device Interface 2.2 (Cisco E-DI).

Cisco E-DI provides a CLI user interface (CLI-UI), a GUI, and an XML programmatic interface (XML PI). Cisco E-DI is used by Enterprise as well as Service Provider customers. It supports configuration for Cisco IOS and CatOS network elements (NEs) and Cisco PIX firewall devices, and applicable services and devices, including L3 MPLS VPNs, Metro Ethernet, select switches and branch office equipment.

For the latest and updated documentation of Cisco Enhanced Device Interface, 2.2, please check Cisco.com:

http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

The following documentation is a part of Cisco E-DI 2.2:

- *Release Notes for Cisco Enhanced Device Interface 2.2 on Windows* - OL-12568-01
- *Release Notes for Cisco Enhanced Device Interface 2.2 on Linux* - OL-12569-01
- *Installation and Setup Guide for Cisco Enhanced Device Interface 2.2 on Windows* - OL-12565-01
- *Installation and Setup Guide for Cisco Enhanced Device Interface 2.2 on Linux* - OL-12566-01
- *User Guide for Cisco Enhanced Device Interface 2.2* - OL-12567-01
- *Programmer's Guide for Cisco Enhanced Device Interface 2.2* - OL-12570-01

## Audience

This guide is designed for system administrators and users who are responsible for the operation of the Cisco E-DI.

# Conventions

This document uses the following conventions:

***Table 1 Conventions***

| Convention | Description |
|---|---|
| ^ or Ctrl | ^ or Ctrl represents the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive. |
| *string* | A string is a nonquoted set of characters. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks. |
| `screen` | Courier plain shows an example of information displayed on the screen |
| **`boldface screen`** | Courier bold shows an example of text that you must enter. |
| < > | Angle brackets show non printing characters, such as passwords. |
| ! | An exclamation point at the beginning of a line indicates a comment line. |
| [ ] | Square brackets show optional elements. |
| {} | Braces group alternative, mutually exclusive elements that are part of a required choice. |
| \| | A vertical bar, also known as a pipe, separates alternative, mutually exclusive elements of a choice. |

**Caution** Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

**Note** Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

**Timesaver** Means the described action saves time. You can save time by performing the action described in the paragraph.

**Tip** Means the information will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

# Cisco E-DI Concepts

Cisco Enhanced Device Interface (Cisco E-DI) provides a comprehensive management interface for Cisco devices. See Figure 1-1. This chapter contains the following information:



## Overview

Cisco E-DI provides interfaces for two main categories of users:

- The human user interacting with network devices through the command line interface (CLI) and the graphical user interface (GUI).
- Management application programs interacting with network devices through a programmatic interface (PI).

Most of the Cisco devices natively provide a comprehensive CLI for a human user to handle all device level management functions. Cisco E-DI builds upon that capability providing value added functions to manage groups of devices conveniently, while keeping the new commands consistent with Cisco IOS CLI.

Cisco E-DI provides an intuitive syntax validation of the commands, easy visual feedback on configurable and operational aspects of multiple devices in the network, and running CLI scripts on groups of devices.

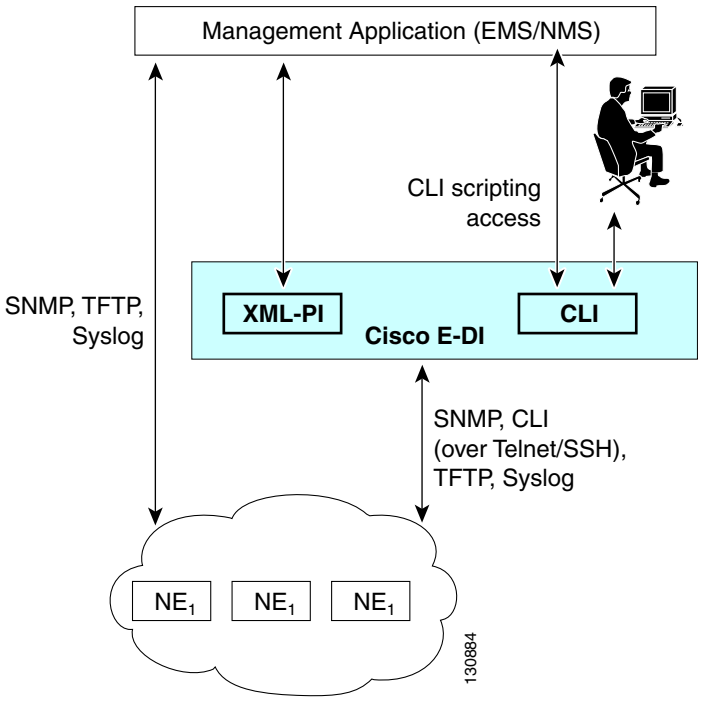
The Cisco E-DI GUI includes the Device Configuration Manager which provides an alternative way to view and edit device configurations. The GUI is a convenient ways of viewing and editing the entire configuration before applying the changes to the device. It gives visual clues to help the user edit the configuration commands.

While CLI scripts and macro commands can provide some programmatic support for managing large networks, the approach can still be cumbersome and unsuitable for comprehensive management of large networks.

Management applications handling multi-vendor devices expect a standards based programmatic interface. Cisco E-DI provides an XML (eXtensible Markup Language) PI based on NETCONF configuration protocol standards. See Figure 1-1.

The supported data model is published through XSD (XML Schema Definitions) files.

***Figure 1-1 Cisco E-DI***




Management functions on Cisco devices can be classified as:

- Configuration, for example **Conf**
- Operational control, for example **EXEC** commands
- Operational data retrieval, for example **Show** commands
- Notifications (alarms and Syslogs)
- Device troubleshooting and debugging
- Device software updates and upgrades

Functionality natively supported on a Cisco device is always available to the Cisco E-DI user.

Cisco E-DI primarily offers an enhanced interface for the following device level tasks:

- Configuring a device through XML PI and CLI
- Implementing EXEC commands on a device through XML PI and CLI
- Viewing a device file system through CLI
- Viewing device events through CLI
- Viewing and modifying device software through CLI
- Viewing device information and status through CLI

Cisco E-DI includes network virtualization for managing multiple devices. Network virtualization allows the user to dynamically group multiple devices into a single entity, and perform any of the tasks on all the selected devices.

A Cisco E-DI server manages a group of devices. However, if a user chooses to deploy multiple Cisco E-DI servers to manage the network, the partitioning of the network and which server will manage what partition of the network, will be the user's responsibility.

Cisco E-DI is agnostic about another Cisco E-DI managing the network.

# Cisco E-DI Features

Cisco E-DI includes the following features:

- XML programmatic interface
- JAVA SDK for XML programmatic interface
- CLI network virtualization
- GUI for:
  - Configuring devices (Device Configuration Manager)
  - Creating command macros to handle device variations (Macro Command creation feature)
  - Analyzing commands (Command Analyzer)
  - Creating a device model/spec file, XML file, and XSD for show commands (Operational Data Model Tool)
  - Creating device-independent CLI models which can be used to generate device-specific Java code (Infrastructure for Virtual Device Model)
- Network management
- Configuration Compliance support
- ACL configuration support
- Session based device authentication
- Platform/OS support
- Configuration file management
- Basic inventory management
- Job scheduling
- Network troubleshooting and diagnostics
- Information synchronization

- Alarm/event handling
- Integral FTP server
- Server management
- Perl scripting capabilities
- Security management
- Color mode configuration

# Types of Users

There are four types of Cisco E-DI users:

- Administrator—Has full access and all privileges, and is considered to be the highest level of access. The default username is **admin**, and password is **admin**.
- Network operator—Can perform any network related operations on Cisco E-DI; cannot modify the configuration or setup information. Multiple network operator accounts are possible, and can be defined by the administrator.
- Read-only user—Has read-only permissions, and cannot modify configurations.
- No access user—The default privilege over the domain's defined device group and the server. Privileges are to restrict any operation on the defined domain.

See Chapter 14, "Maintaining Cisco E-DI" for more details.

# Security in Cisco E-DI

This section includes the following information:



## User Authentication

The AAA server in Cisco E-DI can be configured with TACACS+ or RADIUS protocols.

The Linux shell does user authentication by default. User authentication can also be done through a TACACS+ server or a RADIUS server. These servers can be configured in the server config mode.

When a TACACS+ server or a RADIUS server is configured for user authentication, all the users to be authenticated must be created using the **user** command.

Users can be created with or without a password. If a user is created with a password, they can be authenticated with the local password or the TACACS+/RADIUS password.

*Table 1-1 Commands to Configure the AAA Server for User Authentication*

| Action | Command |
|---|---|
| To configure the AAA server with TACACS+ or RADIUS.<br>• <*A.B.C.D*> is the IP address of TACACS+/RADIUS server<br>• <*encryption-level*> is the encryption level <0-2><br>• <*key-value*> is the shared key value. The shared key configured on Cisco E-DI should match the one configured on the AAA server. | `[SRV:/server] (config)# [no] aa server radius\| tacacs <A.B.C.D> key <encryption-level> <key-value>` |

# Role Based Access Control

Users need to login to Cisco E-DI by specifying a username and password.

When a user attempts to login to Cisco E-DI in an SSH or Telnet session, the user is authenticated. On successful authentication, users are able to access the CLI.

Each user is associated with a domain group. The privileges for the domain group are specified when the domain group is created. For more information about domain groups and control, see "Domain Control" section on page 3-13.

Cisco E-DI provides role based access control at the device level, so that access to an NE is allowed or disallowed based on access privileges configured by the Cisco E-DI administrator.

To enable role based access control, any new user has to be associated with an existing domain group. Each module contains the task information for which it is responsible. Authorization information for each task is maintained in XML files for each privilege level.

This information is loaded at the time the Cisco E-DI server is started.The command will only be implemented if the authorization check is successful.

For example, a Cisco E-DI user can perform a management task on an NE only if:

- The user is in the FULL_CONTROL domain group

  Or

- The NE is one of the devices in the domain group, and the task the user is trying to perform, is permitted in the domain group

# Syslog Events

All logins and configuration changes done in Cisco E-DI are published as Cisco E-DI Syslog events and stored in the database. The events contain the name of the user who logged in successfully. Configuration change events contain the name of the user who made the changes.

External Syslog receivers are able to receive the Syslog events by subscribing for the events. Syslog events can be subscribed to using the Cisco E-DI server configuration command **logging host <IP-ADDRESS>**.

# Device Authentication

Device authentication allows the administrator to choose between a centralized credential model (**non session based device authentication**) and a per user-session credential model (**session based device authentication**). Whichever mode is chosen is applied to all devices in the network.

During installation of Cisco E-DI, the administrator is prompted to choose between session based and non session based device authentication mode. Non-session based device authentication is selected by default. A user can switch between session based and non-session based device authentication mode at any time.

In Cisco E-DI, SNMP read-community and write-community credentials and enable password are shared, and are non-session based irrespective of the device authentication mode.

The administrator must specify the SNMP read community in the credential set. If required, the administrator can use domain grouping to restrict user access to devices. See Groups.

## Non Session Based Device Authentication

Non session based device authentication can be used in an environment where there is no external AAA server.

If the administrator selects non-session based device authentication during installation, Cisco E-DI prompts the administrator to set up the Syslog auto subscription feature.

Cisco E-DI uses credential sets which are centralized (non-session based) device credential stores. The administrator is required to pre-configure Cisco E-DI with the following device information in a credential set:

- SNMP Read Community
- SNMP Write Community (optional)
- Telnet/SSH login username
- Telnet/SSH password
- Enable password
- The transport type used for CLI sessions between Cisco E-DI and the device. (telnet or SSH)

Once these credentials are pre-configured for the managed devices, Cisco E-DI will use them automatically or on demand.

## Session Based Device Authentication

Session based device authentication is the default mode of operation in Cisco E-DI. The user enters the device credentials at logon time.These credentials are automatically set for the user session. This means that the device users should exist in Cisco E-DI for devices to be managed through Cisco E-DI. The user can enter **terminal device-auth** to override the credentials given at login time.

When a network includes an external AAA server such as Cisco Secure Access Control Server, then non-session based device authentication is unsuitable. For these networks, Cisco E-DI provides session based device authentication which requires a user to enter a login and password when managing devices.

The device authentication login and password are valid for the entire duration of the user session, and are used for authenticating all the devices. The session login and password is not stored in Cisco E-DI.

Session based device authentication requires a user to set a login and password in the session in order to run the following commands:

- **diag connectivity**, and variations of this command
- **diag device**
- **config setup**, through the CLI or XML PI
- **commit**, in config setup mode,
- **sync config fg|bg**
- **sync filesystem fg|bg**
- **inventory**
- **connect exec-mode**
- **exec-cmd** *<command>*, through the CLI or XML PI.
- **copy** *<from-device>* *<to-server>*, includes the more command.
- **copy** *<from-server>* *<to-device>*. In this case, the destination filename is either deviceip:running-config or deviceip:startup-config.
- **write [mem]**
- **reload device** *<ipaddress>*

A user can overwrite the credentials stored in the session, in which case any new connections opened to devices from that point on will use the new credentials. The user must re-enter the session login and password if the Cisco E-DI session times out or is disconnected.

Passwords are destroyed from memory as soon as a user session terminates. A user can also explicitly delete passwords from memory by using the **terminal no device-auth** command.

When session based device authentication is enabled, the administrator can configure a central login and password in the credential set that will be used for background configuration and file system synchronizations.

Session based device authentication can be turned on or off during the Cisco E-DI installation. It can also be enabled or disabled at any time by the system administrator using the **[no] device-auth session-based** command.

If the administrator selects session based device authentication, Cisco E-DI automatically sets Syslog auto-subscription to off. The user will be notified that each managed device must be configured to forward the Syslog messages to Cisco E-DI either directly or through a Syslog relay agent.

When session based device authentication is enabled, any login and password configured in the credential sets will be used only for background configuration and file system synchronizations.

# Platform/OS Support

The actual devices, line-cards and OS releases supported by Cisco E-DI are determined and identified by the incremental device update (IDU) process and published on a regular basis.

You can download the device packages from: http://www.cisco.com/cgi-bin/tablebuild.pl/E-DI-2.0. To get the required device package:

1. Check whether the device package is available at this URL: http://www.cisco.com/cgi-bin/tablebuild.pl/E-DI-2.0.
2. If it is present, download the device package. You need to have your Cisco.com user login to download these packages.
3. After downloading the device packages, copy them to the *E-DI Install Location*/Cisco EDI/edi/dist/devpackages directory.

# Communicating With Devices

Cisco E-DI uses SNMP, TFTP, and Telnet or SSH protocols to communicate with devices. Cisco E-DI supports SSH v1.5 and SSH v2. The administrator has the option of choosing Telnet or the required version of SSH.

The user must specify a login, password, and an enable password for the chosen protocol. All device credentials, such as SNMP community strings and CLI passwords, are encrypted and stored in the startup configuration of the Cisco E-DI. See Credential Sets for more details.

Certain operations on a device can be destructive, for example, write erase which will erase the entire contents of flash on a device. Cisco E-DI provides a default list of forbidden commands, and administrators are able to modify the list. In Cisco E-DI, the administrator can define a list of commands which are not allowed to be implemented on any device. See Session Based Device Authentication.

# Network Virtualization

Cisco E-DI includes the concept of network virtualization, where a network (a subnet, a network in a building, a group of devices) is seen as a single virtual device. For more information about groups, see Groups.

# Command Line Interface (CLI) and Prompt

Cisco E-DI allows the user to interact with network devices through the command line interface (CLI). Cisco devices natively provide a comprehensive CLI for a user to handle all device level management functions.

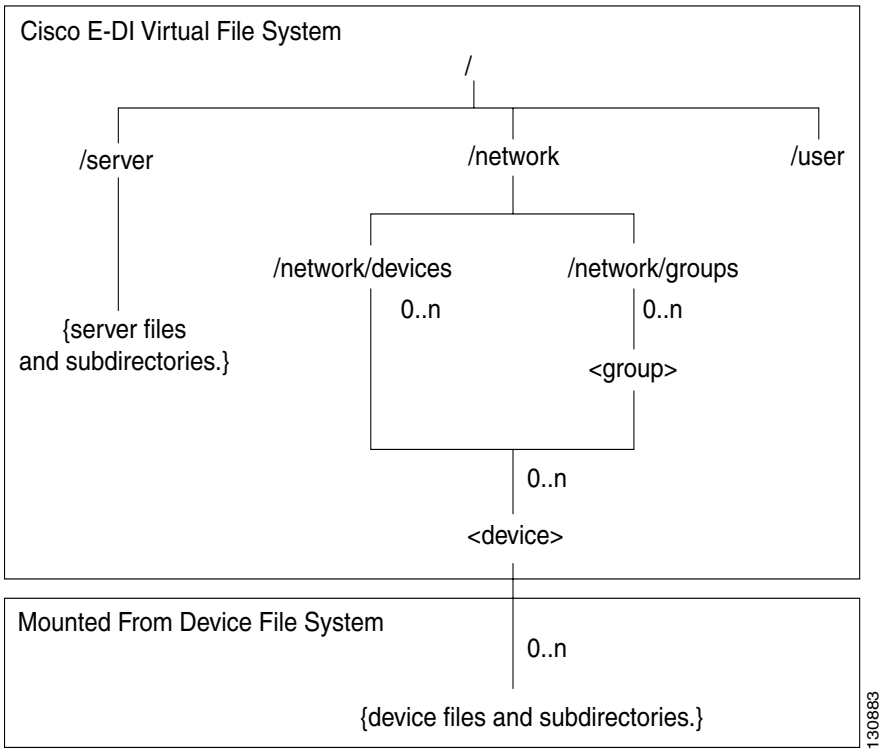
There are three related concepts in Cisco E-DI:

- Command context
- Virtual File System (VFS)—Integrates Cisco E-DI server's file system and the managed device's file system into one directory structure, allowing the user to navigate through the file systems from a single console. See Figure 1-2.
- Command mode

Command context and VFS are related. The command context set commands, **network** and **server**, and VFS directory command **cd** change both the command context and the VFS directory path, and enable navigation within the Cisco E-DI main command. This behavior differs from a traditional operating system's shell.

For example, in UNIX, there is only one command (**cd**) that changes the directory path. See Table 1-2 for examples.

*Figure 1-2 Cisco E-DI Virtual File System*




# Network Mode

In Cisco E-DI setting the command context to network using the **network** command changes the working directory at the same time to **/network**. Cisco E-DI network configuration command mode is used for configuring devices on the network.

This mode contains configuration sub-modes based on the specific device or devices types, and associated software version.

In this mode, operations apply on the devices in the network. The prompt signifies on what sub-set of devices the actions will be performed. In network mode there are two pre-defined sub-modes which in turn have multiple sub-modes.:

- Groups
- Devices

# Server Mode

Setting the command context to server using the **server** command changes the working directory to **/server**. Cisco E-DI server configuration command mode is used for configuring the Cisco E-DI server.

In this mode all server related functions can be performed. For example, use server mode to see all the users and their rights, to configure credential sets and to implement other configuration commands.

# Cisco E-DI Default Prompt

The Cisco E-DI default run-time prompt includes the VFS path. This indicates the path which changed as a result of the command context command. It also shows the present directory as the user navigates through the directory structure to provide more context.

The Cisco E-DI prompt format is as follows:

```
User@Hostname[CommandContext:DirectoryPath]#
User@Hostname[CommandContext:DirectoryPath](CommandMode)#
```

The command context is shown as follows:

- SVR—Server
- NET—Network
- DEV—Device
- GRP—Group of devices

Table 1-2 shows examples of the Cisco E-DI prompt. CLI Command Mode and Command Context details the command context.

To avoid long pathnames in DirectoryPath, paths under /network/devices and /network/groups will have the /network/devices and /network/groups prefix replaced with ~ character. Others are to be shown in their full path.

***Table 1-2 Cisco E-DI Prompt Examples***

| Examples |
|---|
| Welcome to Cisco Management Switch (1.2)<br>Copyright (C) 2005 Cisco System, Inc. All rights reserved.<br><br>[Terminal vty4 Size 25x80]<br><br>admin@hostname[SVR:/]# |
| admin@hostname[SVR:/]# cd server<br>admin@hostname[SVR:/server]# |
| admin@hostname[SVR:/server]# server maintenance<br>admin@hostname[SVR:/server](server-maint)# |
| admin@hostname[SVR:/server]# config t<br>You are entering SERVER configuration mode.<br>admin@hostname[SVR:/server](config)# |
| admin@hostname[SVR:/server]# network<br>You are now in network view.<br>Your present working directory: /network<br>admin@hostname[NET:/network]# |
| admin@hostname[NET:/network]# cd devices<br>admin@hostname[NET:/network/devices]# |
| admin@hostname[NET:/network/devices]# cd 172.16.0.0<br>admin@hostname[DEV:~/172.16.0.0]# |
| admin@hostname[DEV:~/172.16.0.0]# cd disk0:<br>admin@hostname[DEV:~/172.16.0.0/disk0:]# |
| admin@hostname[DEV:~/172.16.0.0]# conf setup<br>You are entering network config-setup mode |

The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

*Table 1-2 Cisco E-DI Prompt Examples (continued)*

| Examples |
| --- |
| admin@hostname[DEV:~/172.16.0.0] (config-setup)# config t<br>You are entering network configuration mode. Number of devices selected: 1<br>Selected device types:<br>----------------------<br>Device Type No. of Version<br>Devices<br>----------------------------------------<br>Cisco7200 1 12.2(14)T2<br><br>admin@hostname[DEV:~/172.16.0.0](config)# |
| admin@hostname[NET:/network]# network group Routers<br>You are now in network view.<br>Your present working directory: /network/groups/Routers/<br>admin@hostname[GRP:~/Routers]# |

# Cisco E-DI User Defined Prompt

Cisco E-DI provides the option for the system administrator to customize the run-time prompt, and f or a user to customize a terminal prompt. See Customizing the Default Prompt.

# CLI

Cisco E-DI NetCLI is the primary user interface to Cisco E-DI and is a CLI editor whose command editing facility is similar to that of Cisco IOS.

To leverage the existing knowledge base in the Cisco user community, Cisco E-DI CLI is Cisco IOS CLI-like, Cisco E-DI NetCLI follows the same basic Cisco IOS CLI rules and behavior, for example, the concept of a **no** command to delete a configuration item.

The Cisco E-DI CLI includes the following features:

- CLI Command Mode and Command Context—Supports various CLI modes and context. Some of the examples of CLI modes are:
  - Main Cisco E-DI command mode
  - Cisco E-DI server configuration mode
  - Cisco E-DI server maintenance mode
  - Device and group configuration command mode
  - Device and group tunneled **EXEC** command mode

  Additionally, a pass-through command is provided to send a single unvalidated EXEC command.
- CLI Color Mode—Color is used for status summary in the CLI prompt and to indicate syntax validity by highlighting the entered command text.
- Filter/Pipe—All commands that produce text output to the screen supports | options to pipe the text output to e-mail, filtering criteria or redirection to a file as follows:
  - append—Appends the data to a file.
  - begin—Begins with the word that matches.
  - email—Sends an email.

  - exclude—Exclude lines that match a pattern.
  - include—Include lines that match a pattern.
  - save—Saves the data to a file.
- CLI User Interface:
  - Supports creation of a minimum of 100 user accounts.
  - Supports a minimum of 20 concurrent active user sessions.

# CLI Command Mode and Command Context

As in Cisco IOS, the Cisco E-DI CLI command mode determines the set of commands available to the user at the prompt.

However, in addition to command modes within the main Cisco E-DI command mode, the CLI also uses **command context** to determine the entity that the command is applied to, whether or not the command is applicable, and if it is applicable, how to interpret the command.

There are six main CLI command modes and the four command contexts within the main Cisco E-DI command mode. The Cisco E-DI prompt indicates the context (Server, Network, Group or Device) and path (Directory).

The six basic CLI modes are:

***Figure 1-3 Main Cisco E-DI command mode***

This is the main menu of the system containing main commands such as directory and file related commands, diagnostics commands, scripting commands, and commands to enter sub-modes. The main Cisco E-DI command mode also includes a subset of device and group **EXEC** commands that are syntax-validated and interpreted and implemented by Cisco E-DI.

The outputs of these commands are generated by Cisco E-DI by interpreting the output generated by the device, not directly by the device itself.

- Device and group configuration setup command mode

  This mode is where all network related configurations are performed. The config-setup mode contains commands for entering into config mode for selected devices or combinations of devices to save, commit, schedule or discard configuration changes.

- Device and group configuration command mode

  Contains device and group configuration commands that are syntax-validated, but not interpreted or processed by Cisco E-DI. This mode is related to the configuration setup command mode. The commands are sent to the device as a group at the end of the configuration session

  This mode contains configuration sub-modes based on the specific device or devices types, and its software version.

- Cisco E-DI server configuration command mode.

  Contains commands for configuring the Cisco E-DI server.

- Cisco E-DI server maintenance command mode.

  Contains commands for maintaining the Cisco E-DI server.

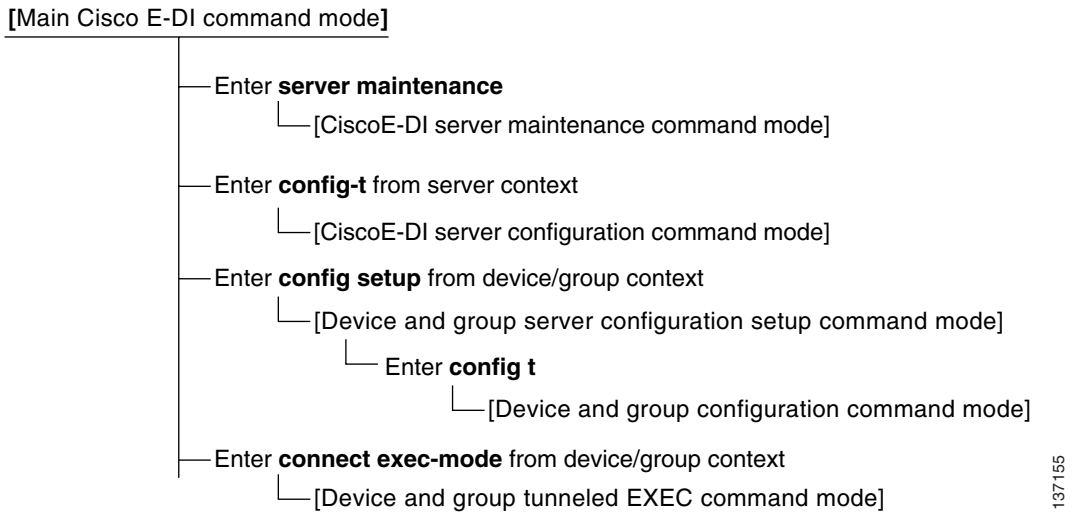
- Device and group tunneled EXEC command mode.

Device and group non-configuration device commands that are syntax-validated, but not interpreted or processed by Cisco E-DI. Commands are immediately sent to the device as soon as they are validated and the output, produced by the device, is shown to the user.

An option to send a single non-syntax-validated EXEC command from the main Cisco E-DI command mode is also provided.

Figure 1-4 shows the hierarchy and relationship of the 6 basic CLI modes.

***Figure 1-4 Hierarchy and Relationship of the CLI Modes***




The four command contexts within the Cisco E-DI main command mode are:

- Server (SVR)

  Context is set to server when the working directory is /, /server and its subdirectories, and /users and its subdirectories.

- Network (NET)

  Context is set to network when the working directory is /network, /network/devices, and /network/groups.

- Device (DEV)

  Context is set to device when the working directory is /network/devices/<device id>.

- Group (GRP)

  Context is set to group when the working directory is /network/devices/<group id>.

The concept of a group is an integral part of Cisco E-DI. For more information, see Grouping, page 3-12. Command context is associated with the Cisco E-DI VFS directory path.

Navigation between command contexts and VFS directories within the Cisco E-DI main command mode is supported by both the network and server command, and by the directory change command **cd**.

Table 1-3 details the configuration submodes available when configuring devices. A list of available device types is displayed when you enter the network configuration mode. Enter [NET:/network] (configure) # ? to display a list of the submodes available for the selected device types.

*Table 1-3 Configuration Submodes*

| Command | Command Mode |
|---|---|
| `[SVR:/server] # cd` | `[SVR:/users/admin] #` |
| `[SVR:/server] # network` | `[NET:/network] #` |
| `[NET:/network] # config s` | `[NET:/network] (config-setup) #` |
| `[NET:/network] (config-setup) # config t` | `[NET:/network] (configure) #` |
| `[NET:/network] (config-setup) # connect exec-mode` | `[NET:/network] (netexec) #` |

# CLI Color Mode

Cisco E-DI CLI color mode enhances CLI usability by coloring the display headings and CLI mode in the prompt. The NE's alarm aggregate status is indicated in the CLI prompt. The color of the prompt indicates the highest alarm severity found in the devices within the scope of the CLI mode, as follows:

- Red—If any one of the devices has a P1 alarm.
- Yellow—If all the devices have P2 and lower alarms.
- Green—When the devices have no alarms on them.

Cisco E-DI color mode has been tested on the following terminal types:

- Putty (open source client for SSH and Telnet)
- Token2 (Open source Telnet Client)
- Windows DOS Telnet application
- Windows Hyperterminal

Additionally, each command typed by the user instantly gets color highlighted to indicate the validity of the command.

For example, if the user enters the word **hostne** for the hostname command, the text will be highlighted blue till the word **hostn** is entered, but as soon as **e** is typed, the word **hostne** will be highlighted red to indicate that there is no matching command for that word.

# Cisco E-DI admin Account

Cisco E-DI provides a pre-defined **admin** account. The name of the account may not be changed by any user, but the password can be changed. Users with FULL_CONTROL access are considered to be Cisco E-DI administrators. Any Cisco E-DI administrator can add more administrators or other user accounts in Cisco E-DI using the CLI commands.

# Cisco E-DI Root Login

Access to the **root** login is fully restricted since the root login and password is disabled.

An incremental root login package that enables root login is available as a patch for debugging and serviceability purposes. On applying this patch, a user can gain root privileges. The purpose of the root login is to allow TAC, or the user with instructions from TAC, to troubleshoot basic Linux functions.

See the *Cisco Enhanced Device Interface 2.2 Installation and Setup Guide* for details about how to obtain patches.

# Graphical User Interface (GUI)

Device Configuration Manager (DCM) of E-DI, is an Eclipse-based GUI tool to view and edit a configuration before applying the changes to the device.

Device Configuration Manager can be used to edit the contents of the startup configuration file and the running configuration file, and apply the configuration to the device. To launch and use DCM, see the topic Launching Device Configuration Manager (DCM). This tool is also known as Config Manager.

Two other tools are available with the DCM suite:

- Macro Command Manager

  Provides a CLI and a GUI interface to create macros across the various device OS versions. Allows you to do network provisioning, using the macro grouping capability.

  To launch and use Macro Command Manager, see the topic Creating and Using Macro Commands.

- Command Translator

  Enables you to translate Cisco Catalyst Operating System (CatOS) configurations to equivalent, supported Cisco IOS configurations.

  To launch and use Macro Command Manager, see the topic Translating Commands Using Command Translator.

# Configuring Multiple Devices

Through the network virtualization feature, Cisco E-DI provides an ability to configure multiple devices with one set of commands. When a user selects multiple devices of different types and/or different OS versions, Cisco E-DI automatically determines the least common denominator set of commands and presents them to the user in typical Cisco IOS-like fashion.

The command is highlighted with an appropriate color to give the user an instant feedback on the validity of a command with the given device/OS selection.

See CLI Color Mode for more information. The user can then press the key combination **Ctrl-G** to view the detailed mapping of a command for any given device type/OS version.

When configuring multiple devices, Cisco E-DI provides interface macros, for example all-fastethernet, all-gigabitethernet. When configuring a single device, Cisco E-DI provides an additional macro for selecting a single interface.

# Syntax Checking

Cisco E-DI maintains the CLI knowledge base for every device family/OS version that it supports. With this knowledge base, Cisco E-DI can perform automatic syntax checking on all user input. Cisco E-DI also internally uses the syntax checking feature to intelligently identify changes between two configurations.

Cisco E-DI also allows the user to select syntax checking of additional options such as OS version, and OS type.

# Credential Sets

Device credentials like login, password, and SNMP community string settings are required for communication with a device. Cisco E-DI combines these credentials into a credential set which specifies the necessary information for Cisco E-DI to communicate to the device. It is assigned to a device when the device is managed.

The behavior of the **login** and **password** commands changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

Credential sets have the following attributes:

- Community strings

  SNMP read and write community strings.

- Login credentials

  Username, password and enable password to Telnet to a device.

- Console server

  Terminal server's IP address and port information for devices accessible through the terminal server.

- Transport type

  Transport options are either Telnet, or SSH v1.5, or SSH v2. This selection is pre-determined by the administrator at the time of managing the device. Choice of communication protocol will not be available to each session.

  The following ciphers are supported for SSH:

  - 3des—Triple-DES cipher. This is the default cipher type for SSH.
  - aes_128—AES cipher (128 bit)
  - aes_192—AES cipher (192 bit)
  - aes_256—AES cipher (256 bit)
  - arcfour—Arc Four cipher (SSH v2 only)
  - blowfish—Blow-fish cipher
  - des—DES cipher (SSH v1.5 only)
  - twofish—Two-fish cipher

  The following modes can be configured for SSH v2:

  - cbc
  - cfb
  - ctr
  - ecb
  - ofb

- Encryption level

  Encryption level of the password. Passwords will always be encrypted when displayed. Users have the option to select an encryption level when specifying a password.

- Based-on

Allows the current credential set to inherit attributes from the credential set that follows this option, except for the defined attributes in the current credential set and the terminal server attribute.

**Note** A default credential set exists with SNMP read community string set to **public**. This set will be used if no other credential set is assigned for a device.

Cisco E-DI uses the attributes defined in the credential set to login to the device, and to perform SNMP operations. A credential set can be assigned to a single device or multiple devices. If there is no credential set assigned to a device, default credential set will be used.

Credential sets can also be used for troubleshooting, where the user specifies the credential set to be used for trying connectivity to the device.

# Groups

Cisco E-DI provides the option to create groups. This can be used to manage groups of devices conveniently. There are the following types of groups:

- Device grouping

  Provide context for the Cisco E-DI CLI operations. There are two types of NE groups:

  - Static Groups—Selecting one or more NE or group.
  - Dynamic Groups—Using a grouping criteria.

- Interface Groups

  Sets of static system-defined groups that combine multiple network interfaces into a single interface which may be used by the user for configuring several interfaces at once. For example, an interface group could be all-Ethernet, or all-fast-Ethernet.

- System Defined Groups

  These groups are pre-defined by the system. They cannot be modified or deleted. Following system groups exist now: AccessPoints, CiscoAP1100, CiscoAP1200, CiscoAP350IOS, Switches, Routers, Firewalls, IDS, CompleteNetwork, and Unknown.

- MyGroup Dynamic Group

  A group created by the user that can contain any managed device based on the context the user chooses. The selection of devices in this group is not persistent, and is lost on exit from the group.

After the NEs are grouped, then the grouped NEs can be placed in a domain group, that is, the administrative domain.

Groups can also be nested within a group.

Groups are fundamental to the concept of network virtualization (see Network Virtualization) where users can dynamically group multiple devices into a single entity, and perform any of the tasks on all the selected devices.

When you select the network mode, operations apply on the devices in the network. The prompt signifies on what sub-set of devices the actions will be performed.

In the network mode there are two sub-modes which in turn have multiple sub-modes. There are two pre-defined sub-modes under the network mode; groups and devices.

# Static Groups

Static groups contain a statically defined set of devices, or other groups which can be static, dynamic or system defined, creating a nested group.

Devices are added to these groups statically. A user can add another static or dynamic group to a static group, to create a nested group. The devices contained in the nested groups are the list of all devices contained in all of the groups included in the nested groups with redundant devices listed only once.

Only managed devices can be added to a static group. Devices can be added to or deleted from a static group.

# Dynamic Groups

Dynamic groups are rule-based. Devices are grouped together based on user-defined rules. The list of devices is dynamically computed based on user-defined rules. Whenever a device is managed, it becomes a part of a dynamic group if it satisfies the rules specified for that group.

Devices cannot be removed from a dynamic group. Devices can be prevented from being added to a group if exclude options are included in the rules for that group. Rule features include:

- Include or exclude capabilities. See Device Capabilities.
- Range of IP addresses
- Device name pattern
- Device type
- Device family

## Device Capabilities

Device capability is a unique name that identifies certain capabilities that a device supports. For example: cdp-mib-supported. Capabilities are used by Cisco E-DI to determine which Cisco E-DI functionalities are applicable to the device.

Table 1-4 lists the capabilities supported by Cisco E-DI:

***Table 1-4 Device Capabilities***

| Name | Device capability |
|---|---|
| bridge-mib-supported | Device capability bridge-mib-supported |
| cdp-enabled | Device capability cdp-enabled |
| cdp-mib-supported | Device capability cdp-mib-supported |
| dot11-ap | Device capability dot11-ap |
| dot11-infrastructure-client-mode | Device capability dot11-infrastructure-client-mode |
| dot11a-radio | Device capability dot11a-radio |
| dot11b-radio | Device capability dot11b-radio |
| dot11g-radio | Device capability dot11g-radio |
| edi-server | Device capability edi-server |
| entity-mib-supported | Device capability entity-mib-supported |

*Table 1-4 Device Capabilities (continued)*

| Name | Device capability |
|---|---|
| firewall | Device capability firewall |
| flash-mib-supported | Device capability flash-mib-supported |
| generic-bridge | Device capability generic-bridge |
| generic-host | Device capability generic-host |
| ids | Device capability ids |
| ios-style-commands | Device capability ios-style-commands |
| l2-switch | Device capability l2-switch |
| l3-router | Device capability l3-router |
| nms-platform | Device capability nms-platform |
| old-cisco-chassis-mib-supported | Device capability old-cisco-chassis-mib-supported |
| os-type-catos | Device capability os-type-catos |
| os-type-ios | Device capability os-type-ios |
| os-type-pixos | Device capability os-type-pixos |
| radio-monitor-mode | Device capability radio-monitor-mode |
| stack-mib-supported | Device capability stack-mib-supported |
| stp-supported | Device capability stp-supported |
| sylog-source | Device capability sylog-source |
| tftp-client | Device capability tftp-client |
| tftp-server | Device capability tftp-server |
| unknown-device-type | Device capability unknown-device-type |
| vpn | Device capability vpn |
| vtp-mib-supported | Device capability vtp-mib-supported |
| vtp-supported | Device capability vtp-supported |

# Interface Groups

Interface group is a static system-defined groups used within a device context. A device context could cover single or multiple devices.

Interface groups allow user to configure multiple interfaces with one set of commands. Interface groups can be used with multiple devices or a single device. The interface grouping feature is only available through the CLI.

Table 1-5 lists the supported interface groups.

*Table 1-5 Interface Groups*

| Name | Description |
|---|---|
| all | Interface group all |
| all-atm | Interface group all-atm |

*Table 1-5 Interface Groups (continued)*

| Name | Description |
|---|---|
| all-bvi | Interface group all-bvi |
| all-dot11 | Interface group all-dot11 |
| all-dot11a | Interface group all-dot11a |
| all-dot11b | Interface group all-dot11b |
| all-dot11g | Interface group all-dot11g |
| all-ethernet | Interface group all-ethernet |
| all-fast-ethernet | Interface group all-fast-ethernet |
| all-ge-wan | Interface group all-ge-wan |
| all-gigabit-ethernet | Interface group all-gigabit-ethernet |
| all-loopback | Interface group all-loopback |
| all-pos | Interface group all-pos |
| all-serial | Interface group all-serial |
| all-vlan | Interface group all-vlan |

# System Defined Groups

There are several pre-defined dynamic groups known as system defined groups, as follows:

- AccessPoints—All Cisco access points in the network
- CiscoAP1100—All Cisco AP1100 devices
- CiscoAP1200—All Cisco AP1200 devices
- CiscoAP350IOS—All CiscoAP350IOS devices
- CompleteNetwork—All devices currently managed by Cisco E-DI
- FireWalls—All Cisco firewalls
- IDS—All Cisco IDS systems
- MyGroup—List of devices currently in user context (for example, if user selects one or more devices with command '**network** *<ip-addr1> <ip-adddr2>*' then both these devices are kept in MyGroup. The contents of MyGroup are specific to user session.
- Routers—All L3 routers
- Switches—All L2 switches
- Unknown—All devices whose type is unknown to Cisco E-DI

# MyGroup Dynamic Group

MyGroup is an ad-hoc dynamic group which is created by the user, and is lost when the user exits the session. MyGroup can be any combination of devices and existing groups.

For example, MyGroup would be created when a command similar to the following is entered:

```
[SVR:/server] (config)# network 172.16.0.202   172.16.0.200 172.16.0.204
```

You can enter `[SVR:/server]#` **`show devices group`** to show the devices in the group.

# Event Handling

Cisco E-DI uses events received from devices, and data collected during polling and inventory, to maintain an accurate representation of the state of the devices and the network.

This data provides the user and higher level applications with an up-to-date view of the health of the device, and alerts the user to configuration changes that are likely to fail. All events received from the network are automatically archived in the database.

Cisco E-DI receives Syslog events directly from NEs, or from Syslog servers in the network. The Syslog event uses the DNS name and IPv4 address to identify the NE. The source IP address can be any interface on a managed device.

If an event is received through two different paths, for example, directly from the NE, and also from a relay agent, Cisco E-DI archives both the events as if they are two different events. As Cisco E-DI performs event collating, duplicate events typically do not cause replicate synchronization actions.

Syslog events are archived in the database according to the timestamp when the event was received by Cisco E-DI.

Cisco E-DI supports the Kiwi Syslog Server.

When creating an action in the Kiwi Syslog Server to forward Syslogs to Cisco E-DI, select the option **Retain the original source address of the message**. If this option is not selected, Syslogs will be forwarded without the device IP address, and Cisco E-DI will drop the forwarded Syslog messages.

Any event received from an unmanaged entity or from unknown relay agent is dropped.

Statistics of the number of relay events received, and events dropped are maintained. You can view these statistics, enter **show server stats**.

CHAPTER 2

# Using Cisco E-DI

This chapter details how to configure and use Cisco E-DI features:



## Connecting to E-DI

You can connect to the E-DI server using any Telnet client. At the command prompt, enter **`telnet`** *hostname port*.

Here, 2323 is the default port.

When asked for user access verification, enter the appropriate username and password. The default administrative username is **`admin`** and default password is **`admin`**.

# Setting up the Terminal

The commands used to set up the terminal are detailed in Table 2-1. You can enter the commands in server or network mode.

***Table 2-1 Commands to Setup the Terminal***

| Action | Command |
|---|---|
| To set the terminal color mode.<br>You can also use the key combination **Ctrl-T** from the server EXEC level to toggle between gray and color modes. | `[SRV:/server\|NET:/network]# terminal color` |
| The terminal display settings can be configured to use either hostname, DNS name, or the IP address of the device. | `[SRV:/server\|NET:/network]# terminal device-id {dns-name \| dns-name-short\| ip \| name}` |
| To define the FTP Authentication credentials.<br>The credentials created using this command are used for downloading a file from an FTP site and for data backup and restore using FTP. | `[SRV:/server\|NET:/network]# terminal ftp-auth username {word}`<br>`Password` |
| To define the HTTP Authentication credentials.<br>The credentials created using this command are used for downloading a file from a website. | `[SRV:/server\|NET:/network]# terminal http-auth username {word}`<br>`Password` |
| To make the session interactive. | `[SRV:/server\|NET:/network]# terminal interactive` |
| To specify the number of lines that are displayed on the terminal. | `[SRV:/server\|NET:/network]# terminal length {0-1} \| {2-256}` |
| When terminal monitor is enabled, any action on the Cisco E-DI server carried out on another session is displayed on the terminal. | `[SRV:/server\|NET:/network]# terminal monitor message filter {word}` |
| To disable the relevant terminal mode. | `[SRV:/server\|NET:/network]# terminal no {color \| http-auth \| interactive \| monitor \| monitor message-filter \| skip-locked \| skip-unauth \| status-codes \| suppress-repeats}` |
| To enable cursor wrap to next line on reaching the end of the line (in some terminals, for example Putty). | `[SRV:/server\|NET:/network]# terminal [no] cursor-wrap` |
| To set the terminal environment variable value. | `[SRV:/server\|NET:/network]# terminal set {word}{word}` |
| To skip all devices locked by some other user. | `[SRV:/server\|NET:/network]# terminal skip-locked` |
| To skip all devices that are not authorized to be included in a task. | `[SRV:/server\|NET:/network]# terminal skip-unauth` |
| To display the status code after command implementation. | `[SRV:/server\|NET:/network]# terminal status-codes` |
| To set the terminal stream control type.<br>The xml-data-channel option converts the terminal from CLI mode to XML mode (NETCONF).<br>See *Cisco Enhanced Device Interface Programmer's Guide, 2.2* for more details on establishing XML sessions with Cisco E-DI. | `[SRV:/server\|NET:/network]# terminal stream-ctl {xml-data-channel {word}}` |
| To turn the toggle options using the Ctrl key on and off. | `[SRV:/server\|NET:/network]# terminal supress-repeats` |

*Table 2-1 Commands to Setup the Terminal (continued)*

| Action | Command |
|---|---|
| To unset the terminal environment variable. | `[SRV:/server\|NET:/network]# terminal unset {word}` |
| To specify the text width displayed on the screen.<br>The default terminal width is 80. The default terminal length is 24. | `[SRV:/server\|NET:/network]# terminal width {16-256}` |
| To format the output of show commands with pre-defined column width (default setting). | `[SRV:/server\|NET:/network]# terminal format-report` |
| To disable the pre-defined column width based formatting for reports. This command is useful in scripting. | `[SRV:/server\|NET:/network]# terminal no format-report` |

# Customizing the Default Prompt

The commands used to customize the default Cisco E-DI prompt are detailed in Table 2-2. The commands can be given in server mode.

*Table 2-2 Commands to Customize the Default Cisco E-DI Prompt*

| Action | Command |
|---|---|
| To customize the default Cisco E-DI prompt. This prompt is configured by the system administrator, and will be applicable for all users. It is saved to the running configuration.<br>The prompt can include characters and function names as follows:<br>• ServerName—Hostname of Cisco E-DI Server<br>• User—Login ID of user<br>• DIR—Current directory (ex: ~/)<br>• ContextType—SRV or GRP or DEV or NET (entire network)<br>• Context—Device IP address/name or Group name (existing prompt component) with status (when color is enabled)<br>• Status—Alarm Code for the context (OK, Offline, P1, P2 .. P5)<br>• DeviceIP—Device IP address (for single device)<br>• DeviceName—Device Hostname (for single device)<br>• PartialDir—Part of the directory ( In device context, “/network/devices/" and "/network/groups/” in the current directory replaced with ~/.)<br>The maximum length of the prompt is 75 characters. Ctrl characters are not allowed.<br>A function is contained within **%{** and **}** in the prompt definition. After the prompt expression is defined the functions are evaluated and displayed in the prompt.<br>Any character that is not enclosed within **%{** and **}** will be displayed in the terminal prompt.<br>For example, if the prompt is customized as **`terminal prompt %{DeviceIp}-on- EDI-%{ServerName}`** and the DeviceIP (1.1.1.1) and ServerName (Dev-1) are the functions to be applied, the customized prompt will be **`1.1.1.1-on-EDI-Dev-1`**.<br>To include a space in the prompt, you should specify the <prompt expression> in double quotes (“ “). | `[SRV:/server] (config)# system prompt <prompt expression>` |
| To clear the customized terminal prompt, and return to the default prompt. | `[SRV:/server]# terminal no prompt` |
| To save the terminal preferences set in the current session to a profile that will be stored in the user’s home directory.<br>Terminal properties like prompt, color, suppress-repeats, width, and length are saved to the profile. Other terminal properties such as auth-type and skip-unauth are not saved. | `[SRV:/server]# terminal save properties` |

*Table 2-2 Commands to Customize the Default Cisco E-DI Prompt (continued)*

| Action | Command |
|---|---|
| To clear the customized prompt, and return to the default Cisco E-DI prompt. | `[SRV:/server] (config)# no system prompt` |
| To customize the default terminal prompt. This prompt is user defined, and applicable for that terminal only. It is valid for that session only. The prompt can include the characters and functions described above.<br>This prompt has the highest priority. It will override the default Cisco E-DI prompt and the system defined prompt. | `[SRV:/server]# terminal prompt <prompt expression>` |

# Keyboard Shortcuts

Table 2-3 gives the keyboard shortcuts available in Cisco E-DI.

*Table 2-3 Keyboard Shortcuts and Associated Actions*

| Shortcut | Action |
|---|---|
| ? | Opens context sensitive help |
| Ctrl A | The cursor goes to the beginning of the line |
| Ctrl B | The cursor moves one character to the left |
| Ctrl C | Discards the current line |
| Ctrl D | Deletes the character at the cursor |
| Ctrl E | The cursor goes to the end of line |
| Ctrl F | The cursor moves one character to the right |
| Ctrl G | Displays the devices selected, the knowledge base applied and the applicability of the command to the devices selected in device configuration mode |
| Ctrl K | Deletes all characters from the cursor to the end of the command line |
| Ctrl N | Returns more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key |
| Ctrl P | Recalls commands in the history buffer, beginning with the most recent command |
| Ctrl R | Refreshes the current line |
| Ctrl T | Toggles between terminal color display |
| Ctrl U | Deletes all characters before the cursor to the beginning of the command line |
| Ctrl W | Deletes the word to the left of the cursor |
| Ctrl X | Deletes all characters before the cursor to the beginning of the command line |
| Ctrl Z | Exit from configuration mode |
| Enter | For paginated messages (more than one page), message scrolls one line up |

*Table 2-3 Keyboard Shortcuts and Associated Actions (continued)*

| Shortcut | Action |
|---|---|
| Space bar | For paginated messages (more than one page), message scrolls one page up (equal to terminal length) |
| Tab | Completes a partial command |

# Cisco E-DI Services

Cisco E-DI includes a number of services, see Table 2-4. To enable these services, see Table 2-5.

You can configure services in Cisco E-DI according to the category of inventory data required, see Table 7-1.

*Table 2-4 Cisco E-DI Services*

| Service | Default | Description |
|---|---|---|
| asset | Enabled | Device asset collection service.<br>Periodically collects information on device hardware assets such as chassis, cards, slot, power-supply, and fans. |
| editor | Enabled | Text editor service for CLI.<br>Allows you to edit and create files on Cisco E-DI using a vi editor. |
| exec-cmd | Enabled | Direct network EXEC command service.<br>Enables implementing commands on a device using **exec-cmd** command. |
| ftp-server | Disabled | FTPD server service.<br>Enables or disables Cisco E-DI accessibility through FTP. |
| perl-scripting | Disabled | Perl scripting service for CLI.<br>Enables implementation of perl scripts using **perl** command. |
| telnet | Disabled | Enables or disables Telnet service.<br>Enables login to the Cisco E-DI server using Telnet. |
| trap-receiver | Enabled | SNMP trap receiver service.<br>Enables the receiving and processing of SNMP traps.<br>E-DI trap service listens on port 162 which is the default port to receive traps. |

You can enable services in Cisco E-DI with these commands. See Table 2-5

*Table 2-5 Commands to Enable Cisco E-DI Services*

| Action | Command |
|---|---|
| To enable the device asset collection service | `[SVR:/server] (config)# service asset` |
| To enable the text editor service for the CLI | [SVR:/server] (config)# **service editor** |

*Table 2-5 Commands to Enable Cisco E-DI Services (continued)*

| Action | Command |
|---|---|
| To enable the direct network EXEC command service<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | [SVR:/server] (config)# **service exec-cmd** |
| To enable the FTP server service | [SVR:/server] (config)# **service ftp-server** |
| To enable perl-scripting for the CLI | [SVR:/server] (config)# **service perl-scripting** |
| To enable the telnet service | [SVR:/server] (config)# **service telnet** |
| To enable the SNMP trap receiver service | [SVR:/server] (config)# **service trap-receiver**<br>E-DI trap service listens on port 162 which is the default port to receive traps. |

# Commonly Used Commands

Table 2-6 details commands which are commonly used in Cisco E-DI.

*Table 2-6 Commonly Used Commands*

| Action | Command |
|---|---|
| To enter the configure setup mode.<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | `config setup` |
| To enter the configure terminal mode. | `config t` |
| To perform various diagnostic activities on the network. | **diag** |
| To download files using HTTP or FTP onto Cisco E-DI. | **download** |
| To exit out of the configuration mode.<br>You can also use Ctrl-Z | `end` |
| To exit from the current configuration view and move to the parent view. | `exit` |
| To find the managed devices that match a certain criteria. | **find** |
| To show help on different topics based on the text input. | **help** |
| To put the discovered devices into the managed state. | **import** |

*Table 2-6 Commonly Used Commands (continued)*

| Action | Command |
|---|---|
| To collect device(s) inventory. Used in network mode.<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | **inventory** |
| To logout of the server. | **logout** |
| To query a DNS server to lookup and find IP address information for a host or device. | **dnslookup** |
| To ping a element in the network using its IP address or name. | **ping** |
| To check the status of management operations in Cisco E-DI when session based device authentication is enabled.<br>This command displays the status of the credentials for performing different management operations. It can be used to find out why an operation is not happening.<br>These credentials are not validated with the device, instead the status indicates whether the required credentials are configured by the user or not. | `show devices manageability` |
| To synchronize the file system, device configuration and archives on the devices and the server. | **sync** |
| To trace a route to a network element using its IP address or name. | **traceroute** |
| To save the server running configuration to start-up configuration. | **write** |

Click **Launch Visual Config Editor** or **Launch File Editor** to open the applications. See Chapter 6, "Configuring Devices" for information about managing configuration files using the GUI.

# Using Session Based Device Authentication

Session based device authentication is used in an environment where there is an external AAA server. This mode requires a user to enter a login and password when running the commands in Table 2-7. The behavior of these commands changes when session based device authentication is enabled, see Table 2-7 for details.

If session based device authentication has been disabled, it can be enabled by entering the following command in server configuration mode:

```
[SVR:/server](config)# device-auth session-based
```

To disable session based device authentication, enter the following command in server configuration mode:

```
[SVR:/server](config)# no device-auth session-based
```

To specify the session credentials after session based device authentication is enabled, enter the following command in either server or network mode:

```
[NET:/network]# terminal device-auth login <login val>
```

**Note** We do not recommend that you change the device authentication mode after you have started managing devices. If you need to change the mode, you should first clear all previous connections, enter the command **clear status connections**. Then change the authentication mode.

*Table 2-7 Command Behavior When Session Based Device Authentication Is Enabled*

| Commands | Command Behavior When Session Based Device Authentication is Enabled |
|---|---|
| In EXEC Mode | |
| **diag connectivity** | If the command is run within a scheduled job, the Telnet/SSH connectivity test fails.<br>When the command is run, the Telnet/SSH connectivity test uses the session's credential set for login and password. The enable password is taken from the credential set used to manage the device. If the session is not configured with device credentials, the following message appears for the login test:<br>`Device credentials are not configured for this session`<br>Configure the device credentials for this session, enter **terminal device-auth** |
| diag device | If the command is run within a scheduled job, the Telnet/SSH connectivity test fails.<br>When the command is run, the Telnet/SSH connectivity test uses the session's credential set for login and password. The enable password is taken from the credential set used to manage the device. If the session is not configured with device credentials, the following message appears for the login test:<br>`Device credentials are not configured for this session`<br>Configure the device credentials for this session, enter **terminal device-auth** |
| **config setup** | If the device credentials for the session are not configured, the following message appears before entering config-setup mode:<br>`%WARNING: System is setup to use session based device authentication. Your current session is not configured with device credentials.`<br>Configure the device credentials for this session, enter **terminal device-auth**<br>If you proceed with the configuration, the commit command will display the following error message:<br>`%System is configured to use session based device authentication. Your current session is not configured with device credentials`<br>Configure the device credentials for this session, enter **terminal device-auth**<br>If the session is configured with device credentials, the commit operation would use the session's credential to establish a Telnet/SSH connection with the device and issue a copy tftp://ediserver/running-config command on the device.<br>In session based device authentication mode, device configuration cannot be scheduled as a job. |

*Table 2-7 Command Behavior When Session Based Device Authentication Is Enabled (continued)*

| Commands | Command Behavior When Session Based Device Authentication is Enabled |
|---|---|
| **sync config {fg\|bg}** | If this command is run within a scheduled job, it will use SNMP Write operation to synchronize the configuration. If the SNMP Write community is not configured, this command will fail.<br>The command uses the session's device credentials to establish a Telnet/SSH connection and downloads the configuration of the device to Cisco E-DI using TFTP transport.<br>If the device credentials for the session are not configured, the command fails with the following message:<br>`%System is setup to use session based device authentication. Your current session is not configured with device credentials.`<br>Configure the device credentials for this session, enter **terminal device-auth** |
| **sync filesystem {fg\|bg}** | If this command is run within a scheduled job, it will fail.<br>The command will use the session's device credentials to establish a Telnet/SSH connection and retrieve the device file system.<br>If the device credentials for the session are not configured, the command fails with the following message:<br>`%System is setup to use session based device authentication. Your current session is not configured with device credentials.`<br>Configure the device credentials for this session, enter **terminal device-auth** |
| **inventory** | There is no change to basic inventory and asset inventory.<br>The inventory command internally issues **sync config** and **sync filesystem** commands, the behavior of those commands within the inventory job is similar to the behavior describe above. |
| **connect exec-mode**<br>**exec-cmd <cmd>** | These commands cannot be run from a scheduled job.<br>These commands use the session's device credentials to establish a Telnet/SSH connection and run the specified command.<br>If the device credentials for the session are not configured, the command fails with the following message:<br>`%System is setup to use session based device authentication. Your current session is not configured with device credentials.`<br>Configure the device credentials for this session, enter **terminal device-auth** |
| **more <device-filename>**<br>**copy <from-device> <to-server>** | If this command is run within a scheduled job, it uses the SNMP Write operation to synchronize downloading the file from the device to Cisco E-DI using TFTP transport. If the SNMP Write community is not configured, this command will fail.<br>The command uses the session's device credentials to establish a Telnet/SSH connection, and downloads the file from the device to Cisco E-DI using TFTP transport.<br>If the device credentials for the session are not configured, the command fails with the following message:<br>`%System is setup to use session based device authentication. Your current session is not configured with device credentials.`<br>Configure the device credentials for this session, enter **terminal device-auth** |

*Table 2-7 Command Behavior When Session Based Device Authentication Is Enabled (continued)*

| Commands | Command Behavior When Session Based Device Authentication is Enabled |
|---|---|
| **copy <from-server> <to-device>** | If this command is run within a scheduled job, it will fail.<br>The command uses the session's device credentials to establish a Telnet/SSH connection and downloads the file from Cisco E-DI to the device using TFTP transport.<br>If the device credentials for the session are not configured, the command fails with the following message:<br>`%System is setup to use session based device authentication. Your current session is not configured with device credentials.`<br>Configure the device credentials for this session, enter **terminal device-auth** |
| **write mem** | If the device credentials for the session are not configured, the command fails with the following message:<br>`%WARNING: System is setup to use session based device authentication.`<br>`Your current session is not configured with device credentials.`<br>`You must use 'terminal device-auth' command to configure device credentials before executing this command.`<br>The command uses the session's device credentials to establish a Telnet/SSH connection and tftp transport to transfer files between Cisco E-DI and the device. |
| **reload device** | This is applicable in the network EXEC mode.<br>If the device credentials for the session are not configured, the command fails with the following message:<br>`%WARNING: System is setup to use session based device authentication.`<br>`Your current session is not configured with device credentials.`<br>`You must use 'terminal device-auth' command to configure device credentials before executing this command.`<br>The command uses the session's device credentials to establish a Telnet/SSH connection to reload the managed device. |
| In Config mode | |
| **login <login>**<br>**password <passwd>**<br>**enable-password <enpassword>** | If the user attempts to configure any of these parameters in credential-set submode, Cisco E-DI will generate the following warning message:<br>`% Warning: This parameter is not applicable when session based device authentication is enabled` |
| **subscribe syslog** | Syslog auto subscription cannot be enabled in session based device authentication mode.<br>When the user enters the **device-auth session-based** command, syslog auto subscription will be turned off.<br>**Note** The subscribe syslog feature will remain off if the user switches the mode back to non-session based authentication. |

# File System Commands

Cisco E-DI creates a virtual file system to represent the file systems on the managed devices. The virtual file system contains server, network and users directories in the root of the file system:

- **/server** directory contains directories and files related to Cisco E-DI such as directories for storing configuration archives, images and temporary files.
- **/network** directory contains the virtual file system representing file systems for all the devices currently managed.

  This is a read-only file system. Files can be read from the devices, but cannot be written or deleted. The file systems of the devices are learned when the device is managed and are kept current with the device whenever a device inventory is performed. The file systems can also be updated with the **sync filesystem** command.
- **/users** directory contains one directory for each user of Cisco E-DI, which can be used to store user specific files.

Table 2-8 details commands to manage the file system.

*Table 2-8 Commands to Manage the File System*

| Action | Command |
|---|---|
| To change the current directory. | `[SVR:/server\|NET:/network]# cd {/}[name{/name/name…..}]` |
| To switch to the server root directory. | `[SVR:/server]# cd /` |
| To switch to the user's home directory. | `[SVR:/server]# cd` |
| To display the current working directory. | `[SVR:/server\|NET:/network]# pwd` |
| To create a directory with a specified name. | `[SVR:/server\|NET:/network]# mkdir /{server/ \| network/} name` |
| To remove the specified directory. | `[SVR:/server\|NET:/network]# rmdir /{server/ \| network/} name` |
| To show the contents of the current directory.<br>If the filesystem service is disabled, the **dir** command under the device context shows the following warning message,<br>Warning: filesystem service is disabled. Enter **sync filesystem fg** to manually synchronize the data. | `[SVR:/server\|NET:/network]# dir` |
| To view the contents of the specified file. | `[SVR:/server\|NET:/network]# more /{server/ \| network/} name` |
| To delete the specified file. | `[SVR:/server\|NET:/network]# delete {/force \| /recursive \| name}` |
| To copy a file.<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | `[SVR:/server\|NET:/network]# copy {source file destination file}` |

*Table 2-8 Commands to Manage the File System (continued)*

| Action | Command |
|---|---|
| To rename a file. | `[SVR:/server\|NET:/network]# rename name` |
| To synchronize the file system on the server with the file system on the device. You can choose to synchronize the device in the background or the foreground.<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | `[NET:/network]# sync filesystem {bg \| fg}` |

# Restarting the Server or a Device

The command to restart the Cisco E-DI device is detailed in Table 2-9.

*Table 2-9 Commands to Restart Devices*

| Description | Command |
|---|---|
| Restart the specified devices. | `[SVR:/server]# reload device ip-address1 [ip-address2……..]` |

CHAPTER 3

# Managing the Network

This chapter details the options available to the system administrator to manage the network by easily adding devices into Cisco E-DI and grouping them for operational use:

- Credential sets—Allows you to specify how to communicate with the managed devices.
- Discovery—Allows you to discover devices before they are managed.
- Static and dynamic device grouping—Provides context for the Cisco E-DI CLI operations.
- Interface grouping—A set of static system-defined groups that combine multiple network interfaces into a single interface which may be used for configuring several interfaces at once.

Cisco E-DI provides session based device authentication for networks where there is an external AAA server. This mode requires a user to enter a login and password when managing devices. See Device Authentication and Using Session Based Device Authentication for more information.

Session based device authentication is disabled by default, and must be enabled before any devices are managed. This can be done by the system administrator during installation, or by entering the following command in server configuration mode:

```
[SVR:/server](config)# device-auth session-based
```

To specify the session credentials, enter:

```
[SVR:/server]# terminal device-auth login <login val>
```

This chapter includes the following information:

- Managing Devices
- Grouping
- Viewing Devices
- Domain Control

# Creating Credential Sets

Device credentials such as login, password, and SNMP community string settings are required for communication with a device. Cisco E-DI combines these credentials into a credential set which specifies the necessary information for Cisco E-DI to communicate to the device.

It is assigned to a device when the device is managed. See Chapter 1, "Cisco E-DI Concepts" for more information about credential sets.

The commands used to create the credential sets are detailed in Table 3-1. The commands are given in server configure credential set mode `[SVR:/server](conf-credential-set)#`.

***Table 3-1 Commands to Create Credential Sets***

| Action | Command |
|---|---|
| Enter credential configuration mode by specifying a credential set name to configure or assign attributes to the default credential set. | `[SVR:/server](config)# credential-set {default \| name}` |
| A new credential set can be created based on an existing credential set. The new credential set inherits the attributes of the existing credential set. | `[SVR:/server] (config)# credential-set [new name] based-on [name]` |
| To select Telnet transport. | `[SVR:/server](conf-credential-set)# transport telnet` |
| To select SSH v1.5 transport.<br>The SSH default is 3des. | `[SVR:/server](conf-credential-set)# transport ssh [cipher] { 3des \| aes_128 \| aes_192 \| aes_256 \| blowfish \| des \| twofish }` |
| To select SSH v2 transport.<br>The SSH default is 3des. Modes are applicable for all ciphers except arcfour. | `[SVR:/server](conf-credential-set)# transport ssh2 [cipher] { 3des \| aes_128 \| aes_192 \| aes_256 \| arcfour \| blowfish \| twofish_128 \| twofish_192 \| twofish_256 } [mode] { cbc \| cfb \| ctr \| ecb \| ofb \|}` |
| To specify the enable password login for Telnet.<br>The behavior of these commands changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | `[SVR:/server](conf-credential-set)# enable-password [{<0-2> name} \| name]`<br><br>`[SVR:/server](conf-credential-set)# password [{<0-2> name} \| name]`<br><br>`[SVR:/server](conf-credential-set)# login [{<0-2> name} \| name]` |
| To specify the read community for SNMP communication. | `[SVR:/server](conf-credential-set)# read-community [{<0-2> name } \| name]` |
| To specify the write community for SNMP communication. | `[SVR:/server](conf-credential-set)# write-community [{<0-2> name} \| name]` |

*Table 3-1 Commands to Create Credential Sets (continued)*

| Action | Command |
|---|---|
| To remove a credential set. | `[SVR:/server](conf)# no credential-set name` |
| To set the value of a command to null, use **no** before the command. | `[SVR:/server](conf-credential-set)# no read-community`<br><br>`[SVR:/server](conf-credential-set)# no write-community`<br><br>`[SVR:/server](conf-credential-set)# no login`<br><br>`[SVR:/server](conf-credential-set)# no password`<br><br>`[SVR:/server](conf-credential-set)# no enable-password`<br><br>`[SVR:/server](conf-credential-set)# no transport` |

The following example shows two credential sets:

```
credential-set default
read-community 2 681D7F137A19
write-community 2 681D7F137A19
login Cisco
password 2 573E4D2E41
enable-password 2 286B0271127D
transport telnet

credential-set Switch
read-community 2 681D7F137A19
write-community 2 681D7F137A19
login switch
password 2 7F127719
enable-password 2 7F127719
transport telnet
```

Sample credential set created using the **based-on** option:

```
credential-set <new name> based-on <name>
transport ssh
```

The credential set <new name> has all the attributes of the credential set <name> except for the transport type which is SSH instead of telnet as in <name>.

# Assigning a Credential Set

The attributes defined in a credential set are used to login to a device, and to perform SNMP operations.

A credential set can be assigned to a single device or multiple devices. If there is no credential set assigned to a device, the default credential set will be used.

Credential sets can also be assigned to a group of devices using the ip-range command.

**Note** If a credential set is assigned to a device using the manage device command and also using the ip-range, the credential set specified in the manage device command will be used.

The commands used to manage the credential sets are detailed in Table 3-2.

*Table 3-2 Commands to Manage Credential Sets*

| Action | Command |
|---|---|
| To assign a pre-defined credential set to a device. If no credential set is specified, the default credential set is used. | `[SVR:/server](config)# manage device ip_address/dns-name [credential-set name]` |
| To remove a device from the managed list. | `[SVR:/server](config)# no manage device ip_address` |
| To assign a pre-defined credential set to a group of devices, between a specified IP range.<br>• If no credential set is specified, the default credential set is used.<br>• If no name is specified, the default is taken as the name of the list. | `[SVR:/server](config)# ip-range {1-10000} from_ip_address to_ip_address credential-set name` |
| The auto-manage option allows any discovered devices to be added to the managed list automatically.<br>If no name is specified, the default is taken as the name of the list. | `[SVR:/server](config)# ip-range {1-10000} from_ip_address to_ip_address credential-set name [auto-manage]` |
| To remove the IP range specified by the index parameter. | `[SVR:/server](config)# no ip-range {1-10000}` |

# Credential Sets in a Non Session Based Device Authentication Environment

If the administrator selects non session based device authentication during installation, Cisco E-DI uses credential sets which are centralized (non session based) device credential stores.

Table 3-3 lists the protocols and credentials used in non session based device authentication mode.

See Device Authentication, page 1-6 for more details.

*Table 3-3 Protocols and Credentials Used in Non Session Based Device Authentication Mode*

| Feature | Primary Transport/Credentials | Secondary Transport/Credentials |
|---|---|---|
| Discovering the network | Requires SNMP read access to the devices.<br>Credential used—SNMP read community | |
| Collecting NE basic inventory | Requires SNMP Read access to the devices.<br>Credential used—SNMP read community | |
| Collecting NE file system information | Retrieved through Telnet/SSH CLI.<br>Credentials used—login, password, enable password.<br>Credential used—SNMP read community | Retrieved through SNMP READ<br>Credential used—SNMP read community |

*Table 3-3 Protocols and Credentials Used in Non Session Based Device Authentication Mode (continued)*

| Feature | Primary Transport/Credentials | Secondary Transport/Credentials |
|---|---|---|
| Archiving NE configuration | If SNMP write community is configured on Cisco E-DI, the **copy running** *<tftp://ediserver>* command is issued through SNMP write operation (CONFIG COPY MIB).<br>The device uploads the configuration through TFTP.<br>Credential used—SNMP write community | A Telnet/SSH connection is opened and the **copy running** *<tftp://ediserver>* command is issued through CLI.<br>The device uploads the configuration through TFTP.<br>Credentials used—login, password, enable password |
| Retrieving the content of NE files | If SNMP write community is configured on Cisco E-DI, the **copy** *<file> <tftp://ediserver>* command is issued through SNMP write operation (CONFIG COPY MIB).<br>The device uploads the configuration through TFTP.<br>Credential used—SNMP write community | A Telnet/SSH connection is opened and the **copy** *<file> <tftp://ediserver>* command is issued through CLI.<br>The device uploads the configuration through TFTP.<br>Credentials used—login, password, enable password |
| Running EXEC commands on NEs using exec-cmd, connect exec-mode and XMLPI | A Telnet/SSH connection is opened and command is run through CLI.<br>Credentials used—login, password, enable password | |
| Configuring NEs through NetCLI/XMLPI | Configuration data is saved to a file on Cisco E-DI.<br>If SNMP write community is configured on Cisco E-DI, the **copy** *<tftp://ediserver>* **running** command is issued through SNMP write operation (CONFIG COPY MIB).<br>The device downloads the configuration through TFTP.<br>Credential used—SNMP write community | Configuration data is saved to a file on Cisco E-DI.<br>A Telnet/SSH connection is opened and the **copy** *<tftp://ediserver>* **running** command is issued through CLI.<br>The device downloads the configuration through TFTP.<br>Credentials used—login, password, enable password |

# Credential Sets in a Session Based Device Authentication Environment

Cisco E-DI provides session based device authentication which requires a user to enter a login and password when managing devices. The device authentication login and password are valid for the entire duration of the user session, and are used for authenticating all the devices.

In session based device authentication mode:

- For system initiated tasks or scheduled tasks—All credentials used for Cisco E-DI to device communication are from the central credential set, not from the session credential set.
- For user initiated tasks—SNMP credentials and the enable password are from the central credential set, and the Telnet login and password are from the session.

Table 3-4 lists the protocols and credentials used in session based device authentication mode.

See Device Authentication, page 1-6 for more details.

*Table 3-4 Protocols and Credentials Used in Session Based Device Authentication Mode*

| Feature | Primary Transport/Credentials | Secondary Transport/Credentials |
|---|---|---|
| Discovering the network | Requires SNMP read access to the devices.<br>Credential used—SNMP read community | |
| Collecting NE basic inventory | Requires SNMP Read access to the devices.<br>Credential used—SNMP read community | |
| Collecting NE file system information | Retrieved through Telnet/SSH CLI if user initiated.<br>Credentials used—login, password, enable password. | |
| Archiving NE configuration | If the configuration archive is system initiated, and if SNMP write community is configured on Cisco E-DI, the **copy running** *<tftp://ediserver>* command is issued through SNMP write operation (CONFIG COPY MIB).<br>The device uploads the configuration through TFTP.<br>Credential used—SNMP write community<br>For user initiated configuration archival SNMP write is not used (see secondary credentials). | A Telnet/SSH connection is opened and the **copy running** *<tftp://ediserver>* command is issued through CLI.<br>The device uploads the configuration through TFTP.<br>Credentials used—login, password, enable password |
| Retrieving the content of NE files | If the task is system initiated, and if SNMP write community is configured on Cisco E-DI, the **copy** *<file> <tftp://ediserver>* command is issued through SNMP write operation (CONFIG COPY MIB).<br>The device uploads the configuration through TFTP.<br>Credential used—SNMP write community<br>For user initiated configuration archival SNMP write is not used (see secondary credentials). | A Telnet/SSH connection is opened and the **copy** *<file> <tftp://ediserver>* command is issued through CLI.<br>The device uploads the configuration through TFTP.<br>Credentials used—login, password, enable password |

*Table 3-4 Protocols and Credentials Used in Session Based Device Authentication Mode (continued)*

| Feature | Primary Transport/Credentials | Secondary Transport/Credentials |
|---|---|---|
| Running EXEC commands on NEs using exec-cmd, connect exec-mode and XMLPI | A Telnet/SSH connection is opened and command is run through CLI.<br>Credentials used—login, password, enable password | |
| Configuring NEs through NetCLI/XMLPI | Configuration data is saved to a file on Cisco E-DI.<br>A Telnet/SSH connection is opened and the **copy** *<tftp://ediserver>* **running** command is issued through CLI.<br>The device downloads the configuration through TFTP.<br>Credentials used—login, password, enable password | |

# Comparing Credential Sets in a Non Session Based and Session Based Device Authentication

Table 3-5 details and compares the way that components in a credential set function in non session based device authentication and session based device authentication modes.

See Device Authentication, page 1-6 for more details.

*Table 3-5 Comparing the Credentials Used in Non Session Based and Session Based Device Authentication*

| Type of Credential | Non Session Based Mode | Session Based Mode |
|---|---|---|
| SNMP read community | Uses the read community of the credential set configured in the running-config. This can be configured on an individual device basis.<br>Users with at least read-access, can see this credential in an encrypted form in the Cisco E-DI running-config and startup-config. | |
| SNMP write community | Uses the write community of the credential set configured in the running-config. This can be configured on an individual device basis.<br>Users with at least read access, can see this credential in an encrypted form in the Cisco E-DI running-config and startup-config. | |
| Transport Type: Telnet or SSH.<br>(This is not a credential) | Uses the transport field of the credential set configured in the running-config. This can be configured on an individual device basis. | |
| CLI login | Uses the login field of the credential set configured in the running-config. This can be configured on an individual device basis.<br>Users with at least read access, can see this credential in an encrypted form in the Cisco E-DI running-config and startup-config. | Uses the login set in the **terminal device-auth** command by the user in the session. The same login applies to all the devices.<br>The login is stored only in Cisco E-DI memory. It is not visible to any user in any form. |

*Table 3-5 Comparing the Credentials Used in Non Session Based and Session Based Device Authentication*

| Type of Credential | Non Session Based Mode | Session Based Mode |
|---|---|---|
| CLI password | Uses the password field of the credential set configured in the running-config. This can be configured on an individual device basis.<br>Users with at least read access, can see this credential in an encrypted form in the Cisco E-DI running-config and startup-config. | Uses the password set in the **terminal device-auth** command by the user in the session. The same password applies to all the devices.<br>The password is stored only in Cisco E-DI memory. It is not visible to any user in any form. |
| CLI enable password | Uses the enable-password field of the credential set configured in Cisco E-DI running-config (can be configured on a per-device basis)<br>Users with at least read access, can see this credential in an encrypted form in the Cisco E-DI running-config and startup-config. | |

# Device Discovery

Basic network discovery is required primarily in situations where Cisco E-DI is deployed without a management application. Discovery is also useful in cases where a non-Cisco management application is deployed in conjunction with Cisco E-DI, and it lacks adequate discovery capabilities.

Table 3-6 gives the commands required to set up device discovery. Devices need to be discovered first before they are managed.

**Note** Discovery can only be triggered from the CLI.

Two mechanisms for discovery are provided:

- Cisco Discovery Protocol (CDP)
- SNMP sweep

Both these mechanisms require that Cisco E-DI have SNMPv1/v2c read access to the NE. Discovered devices are not automatically managed. Devices need to be selected from the discovered list to be managed by Cisco E-DI.

Discovery with a specified frequency can be scheduled.

This section includes the following information:

- Setting Up Device Discovery
- Discovering Devices
- Displaying and Importing Discovered Devices

## Setting Up Device Discovery

For a CDP based discovery, a seed IP address has to be provided to start discovering the network. Multiple seed addresses can also be specified to make discovery quicker.

A maximum hop count/distance of any discovered device from the seed IP addresses can be specified. The maximum hop count is 10. If no hop count is specified, a default value 1 is used and the hop count is the same for all the seeds specified.

Discovery is performed starting from the seed IP addresses specified till all the devices are discovered or the hop count is reached. In server configure mode, discovery can be scheduled with a list of seed IP addresses, hop count and repetition frequency.

If the discovered devices have multiple IP addresses, typically only one of those IP addresses is meant for management. When Cisco E-DI has to choose one of the IP addresses for device identification and management, and the configuration command **discovery use-mgmt-ip-address** is enabled, it uses the following criteria to determine the management interface address:

1. If a loopback IP address (interface) is configured then this is the preferred management IP address.
2. If a device has multiple loopback IP addresses (interfaces), the first address that gets resolved to a hostname is the management IP address.
3. If a loopback IP addresses cannot be resolved then the preferred IP address is the first configured loopback IP address (based on the ifIndex value).
4. If none of the above rules apply, the preferred IP address is the first configured IP address in the device (based on ifIndex value).

***Table 3-6 Commands to Setup Device Discovery***

| Action | Command |
|---|---|
| To enter the discovery configuration mode. | `[SVR:/server](config)# discovery` |
| To find the devices preferred management IP address during discovery.<br>This option is disabled by default. | `[SVR:/server](config)# discovery use-mgmt-ip-address` |
| To specify the seed IP addresses to be used. | `[SVR:/server](conf-disc)# seed ip_address1 {ip_address2, ….}` |
| To specify a hop count to use. The default value is 1. | `[SVR:/server](conf-disc)# hopcount {number}` |
| To specify a repetition frequency in either minutes or hours.<br>The repetition frequency must be set for a discovery job to run. | `[SVR:/server](conf-disc)# repeat frequency {hours number \| minutes number}` |
| To remove the specified seed IP address, or all IP addresses if no IP address specified. | `[SVR:/server](conf-disc)# no seed {ip_address1, ip_address2, ….}` |
| To remove the specified hop count. | `[SVR:/server](conf-disc)# no hopcount {number}` |
| To disable repetition. | `[SVR:/server](conf-disc)# no repeat frequency {hours number\| minutes number}` |

# Discovering Devices

Table 3-7 details how to start the discovery process.

*Table 3-7 Commands to Start Discovery*

| Action | Command |
|---|---|
| To discover all devices with CDP enabled using the CDP mechanism You need to specify single or multiple seed IP addresses and the hop count to be used.<br>The default hop count is 1. | `[SVR:/server]# discover cdp seed_ip_address [seed_ip_address2 ….] [hopcount number]` |
| To discover all devices using SNMP scan. For an SNMP based discovery, a range of IP addresses is specified.<br>The discovery process begins with the lower address in the range and terminates at the higher address of the range. | `[SVR:/server]# discover snmp-scan ip_address1 ip_address2` |

Any discovery, either scheduled using the configure mode or manually run in the exec mode is implemented in the background. Each discovery job is given a unique task id and the status can be checked using the show discovery command.

# Displaying and Importing Discovered Devices

Table 3-8 gives the commands required to display and import the discovered devices.

*Table 3-8 Commands to Show and Import Discovered Devices*

| Action | Command |
|---|---|
| To show the discovery history for all discovery jobs and the list of devices discovered | `[SVR:/server]# show discovery history` |
| To list all the devices that have been discovered so far and their current status. | `[SVR:/server]# show discovery devices-discovered` |
| To list all the devices that have been discovered for a given discovery job. | `[SVR:/server]# show discovery devices-discovered [task-id]` |
| To list all devices that have been discovered, with their preferred management IP address that has been determined. | `[SVR:/server]# show discovery devices-discovered mgmt-ip-binding` |
| To show discovery task history for a specific discovery job. | `[SVR:/server]# show discovery history [task-id]` |
| To show the discovery task history about the date/time of implementation and number of devices discovered | `[SVR:/server]# show discovery task-history` |
| To clear discovery history related information. | `[SVR:/server]# clear discovery history` |
| To clear the discovered devices list. | `[SVR:/server]# clear discovery devices-discovered` |
| To import all the devices discovered which are currently un-managed, and set them to managed state. | `[SVR:/server]# import devices from-discovered-list all` |

*Table 3-8 Commands to Show and Import Discovered Devices (continued)*

| Action | Command |
|---|---|
| To import the devices selectively.<br>All devices with a manageable state are displayed in the discovery history. Select **y** to manage the device or **n** to skip the device.<br>Select **q** to quit. | `[SVR:/server]# import devices from-discovered-list` |
| To import devices from an XML or CSV seed file. | `[SVR:/server]# import devices from-seed-file filename` |
| To import all devices. | `[SVR:/server]# import devices from-seed-file all` |
| To select the management IP address to be used for device discovery. See Setting Up Device Discovery. | `[SVR: /server](config)# discovery use-mgmt-ip-binding` |
| To show the discovered devices, and the management IP addresses that are identified for those devices. | `[SVR: /server](config)# show discovery devices-discovered mgmt-ip-binding` |

# Managing Devices

Cisco E-DI will only establish connections to NEs that are in the managed device list. Cisco E-DI will reject sessions directed to any unmanaged device and display the following error, %no such managed device exists.

After it starts managing the device, Cisco E-DI to NE communication is independent of any management station to Cisco E-DI communication, and Cisco E-DI manages the device until it is stopped.

**Note** You can clear all previous connections, enter the command **clear status connections**.

All the management tasks can be performed through CLI commands. When Cisco E-DI starts managing an NE, it stores the NE identification information and additional inventory information in the system database.

After device information is located, Cisco E-DI selects a data model from its device package using the following criteria:

- It ensures that the data model's device family matches the target NE's device family.
- For software version, Cisco E-DI tries to find the exact match. If the exact match cannot be found, then it will find the nearest version of the OS knowledge base from the available pool.
- If the NE's OS version is lower than any available OS version then, the lowest available knowledge base version is selected.

You can start managing a device when a credential set has been applied to the device. See Table 3-2.

# Grouping

Cisco E-DI provides the option to create groups. This can be used to manage groups of devices conveniently. See Chapter 1, "Cisco E-DI Concepts" for a detailed explanation of groups in Cisco E-DI.

Table 3-9 details the commands used to manage static groups, and Table 3-10 details the commands to manage dynamic groups.

***Table 3-9 Commands to Manage Static Groups***

| Action | Command |
|---|---|
| To create a static group.<br>The group name can have no more than 40 characters. | `[SVR:/server] (config)# static-group group-name` |
| To enter static group configuration mode. | `[SVR:/server](config)# static-group name` |
| To include a device or a group of devices or any other group static (other than itself), dynamic or system-defined. | `[SVR:/server](conf-static-group)#include {device ip_address \| group name}` |
| To remove the static group. | `[SVR:/server](config)# no static-group name` |
| To remove a specific device or group. | `[SVR:/server] (conf-static-group)# no include {device ip_address \| group name}` |

***Table 3-10 Commands to Manage Dynamic Groups***

| Description | Action |
|---|---|
| To create a dynamic group.<br>The group name can have no more than 40 characters. | `[SVR:/server] (config)# dynamic-group group-name` |
| To enter dynamic group configuration mode. | `[SVR:/server] (config)# dynamic-group name` |
| To specify a rule to be either included or excluded.<br>See Table 1-4 for device capability options. | `[SVR:/server](conf-dynamic-group)# capability (device-capability)* {include \| exclude}` |
| To specify a range of IP addresses to be included into this group. | `[SVR:/server](conf-dynamic-group)# ip-range index from_ip_address to_ip_address` |
| To specify a devicename to be included into this group | `[SVR:/server](conf-dynamic-group)# devicename contains name-pattern` |
| To specify a devicetype name to be included into this group | `[SVR:/server](conf-dynamic-group)# devicetype **devicetype-name` |
| To remove the dynamic group. | `[SVR:/server](config)# no dynamic-group name` |
| To remove a capability rule.<br>See Table 1-4 for device capability options. | `[SVR:/server](conf-dynamic-group)# no capability device-capability` |
| To negate the ip-range rule. | `[SVR:/server](conf-dynamic-group)# no ip-range index` |
| To negate devicename rule | `[SVR:/server](conf-dynamic-group)# no devicename contains name` |
| To negate devicetype rule | `[SVR:/server](conf-dynamic-group)# no devicetype device-type` |

Sample dynamic group configuration in the running config file:

```
dynamic-group Name
    capability cdp-enabled include
    capability edi-server exclude
    ip-range 1 172.16.0.1 172.16.0.15
    devicename contains ap
!
dynamic-group AllRouters
    capability l3-router include
!
dynamic-group AllCisco2600Routers
    devicefamily Cisco2600
!
dynamic-group AllCisco2621Routers
    devicetype Cisco2621
!
static-group SwitchesAndRouters
    include device 172.16.0.1
    include device 172.16.0.5
    include group Switches
    include group AllRouters
!
dynamic-group AllCiscoIOS
    capability os-type-ios include
!
```

# Viewing Devices

After the groups are defined, use the commands in Table 3-11 to view the groups and devices that belong to the group.

When a device is managed, basic information like the device name, software version, type, capabilities are stored in the database. This information changes whenever inventory is performed on the device.

When the server is reloaded, the information stored in the database is loaded before an inventory is performed on the device.

*Table 3-11 Commands to View Devices*

| Action | Command |
|---|---|
| To display all the available groups. | `[SVR:/server]# show groups` |
| To display devices that belong to a specific group. | `[SVR:/server]# show devices [group name]` |
| To enter the group specified to perform network level operations. | `[SVR:/server]# network [group name]` |

# Domain Control

Domain control is a mechanism where a user can perform restricted or controlled operations on NEs grouped under one or more domains with associated privilege levels.

A domain group can consist of multiple groups with individual privileges. See Chapter 4, "Managing Security," for more information about user security and roles. Server privileges are mandatory, with the default privilege level being **NoAccess**.

A user can be assigned a domain group so that operations are restricted to the devices and privileges set in the domain group. When you invoke a task, Cisco E-DI performs the task only on the devices that you have privileges for. If a device belongs to more than one device group, the matching entry will be evaluated and the appropriate privileges are enforced.

There are two pre-defined domain groups that allow the administrator to easily configure initial user privileges:

- FULL_CONTROL group allows all possible network and server privileges.
- NO_CONTROL domain group allows no actions in any context.

Unless explicitly assigned, a domain group will have no server and network privileges. When a domain group is deleted, the user assigned to that domain group will be assigned to a NO_CONTROL group. The user will be reassigned to the group if it is added again.

***Table 3-12 Commands to Manage Domain Groups***

| Action | Command |
|---|---|
| To configure a domain group by name. | `[SERVER](config)# domain-group domain-groupname` |
| To include a device group by index and privilege level. Administrator option can only be obtained by using the FULL_CONTROL domain group. | `[SERVER](conf-domain)# device-group index device-groupname privileges {NetOperator \| NoAccess \| ReadOnlyUser}` |
| To assign server privilege level. Administrator privileges can only be obtained with the FULL_CONTROL domain group. | `[SERVER](conf-domain)# server privileges {NoAccess \| ReadOnlyUser}` |
| To exclude a device group by index and privilege level. | `[SERVER](conf-domain)# no device-group index {device-groupname \| [privileges [NetOperator \| NoAccess \| ReadOnlyUser] ]}` |
| To assign a domain group to a user. | `[SERVER](conf)# user username domain-group {domain-groupname \| [FULL_CONTROL \| NO_CONTROL] {password [ 0 \| 7 ] password}` |

Sample domain group configuration file:

```
dynamic-group BLDG-2
ip-range 1 192.168.3.1 192.168.3.254
!
dynamic-group BLDG-1
ip-range 1 192.168.2.1 192.168.2.254
!
static-group DALLAS
Include device 192.168.2.5
include group CiscoAP1100
!
domain-group LimitedControl
device-group 1 BLDG-2 privileges NoAccess
device-group 2 BLDG-1 privileges ReadOnlyUser
server privileges NoAccess
!
domain-group DALLAS-Admin
device-group 1 DALLAS privileges NetOperator
server privileges ReadOnlyUser
!
user john domain-group LimitedControl password 7 bdMWc9Axpq9HM
user ann domain-group DALLAS-Admin password 7 bdqE0050W3Qaw
```

CHAPTER 4

# Managing Security

The Cisco E-DI security features are described in detail in Security in Cisco E-DI, page 1-4.

Security in Cisco E-DI also includes the following features:

- Locking a Device
- Monitoring Changes in the Network

## Locking a Device

Device locking prevents multiple users making concurrent changes to a device by limiting the write access to the owner of the lock. As long as the lock is held by you, all the other users will only have read access for the locked NEs. An administrator can override the locks, and clear them when desired.

A device will be locked as long as the user intends to hold it. Locks can be cleared when the user intends to relinquish the control of the entity.

A device lock does not prohibit configuration read access.

Table 4-1 details the commands used for working with device locking.

Device locks are one of the features that can be set up in the Cisco E-DI XML Programmatic Interface. See the *Cisco Enhanced Device Interface Programmer's Guide, 2.2* for more details.

***Table 4-1 Commands to Lock Devices***

| Action | Command |
|---|---|
| To create a server lock. | `[SVR:/server]# lock reason text {message, message ..}` |
| To lock an individual device preventing any other user making any changes to the device. | `[NET:/network] (network ip_address)# lock reason text (message, message ..}` |
| To lock all the devices simultaneously at the network level, preventing any other user making any changes to the devices. | `[NET:/network]# lock reason text {message, message ..}` |
| To lock all devices in a group simultaneously to prevent any other user making any changes to the devices; | `[NET:/network] (network group name)# lock reason text message, message ..}` |
| To view all the locks currently held in the current context. | `[SVR:/server]# show locks` |

*Table 4-1 Commands to Lock Devices (continued)*

| Action | Command |
|---|---|
| To clear all the locks currently held in the current context. Use the option override to clear the locks held by other user (requires administrator privileges). | `[SVR:/server]# clear lock [ override ]` |
| To skip all devices locked by some other user, while performing any network level operations. | `[SRV:/server\|NET:/network]# terminal skip-locked` |

# Monitoring Changes in the Network

The network administrator can monitor changes performed on the network through Cisco E-DI. Each user session is monitored, and all activities are logged against a pre-defined priority level (see Table 4-2).

All the tasks that can be performed on a Cisco E-DI server go through a change-log management system which checks the task's priority and logs it into the database. Detailed information about the task, the user, and the commands used to perform the task are logged.

You can configure what tasks should be logged based on a configuration setting. See Table 4-3.

*Table 4-2 Task Priorities*

| Domain | Task Name | Priority Level |
|---|---|---|
| Any | View Devices | 3 |
| Any | View Alarms | 3 |
| Any | View Events | 3 |
| Any | XML Connection | 3 |
| Network | View Interfaces | 3 |
| Any | View Locks | 4 |
| Network | Show Network Connections | 4 |
| Network | View Network Reports | 4 |
| Server | View Server Reports | 4 |
| Server | View Server Lines | 4 |
| Server | Read Server Files | 4 |
| Any | Raise Alarm | 5 |
| Network | View Network Configuration | 5 |
| Network | Read Network Files | 5 |
| Server | View Server Config | 5 |
| Server | View Server History | 5 |
| Server | View Server Logs | 5 |
| Server | Modify Server Files | 5 |
| Network | Update Network Locks | 6 |
| Network | Implement Network Diagnostics | 6 |

*Table 4-2 Task Priorities (continued)*

| Domain | Task Name | Priority Level |
|---|---|---|
| Server | Update Server Lock | 6 |
| Server | Delete Server Files | 6 |
| Server | Backup Database | 6 |
| Server | Discover Devices | 6 |
| Network | Update Network Locks (Override) | 7 |
| Network | Collect Inventory From Devices | 7 |
| Network | Clear Network Reports | 7 |
| Network | Connect Exec-Mode To Devices | 7 |
| Network | Clear Network Events | 7 |
| Network | Clear Network Alarms | 7 |
| Network | Clear Network History | 7 |
| Network | Network Debug Logging | 7 |
| Server | Update Server Lock (Override) | 7 |
| Server | Clear Server Events | 7 |
| Server | Clear Server Alarms | 7 |
| Server | Clear Server Lines | 7 |
| Network | Change Network Configuration | 8 |
| Network | Change Network Configuration (From Terminal) | 8 |
| Network | Write Network Files | 8 |
| Server | Clear Server Logs | 8 |
| Server | Clear Server History | 8 |
| Network | Delete Network Files | 9 |
| Network | Restart Network Devices | 9 |
| Network | Install Software on Devices | 9 |
| Network | Clear Network Connections | 9 |
| Server | Clear Database | 9 |
| Server | Restore Database | 9 |
| Server | Change Server Configuration | 9 |
| Server | Restart Server | 9 |
| Server | Server Maintenance | 9 |

*Table 4-3 Commands to Setup Change Logs*

| Action | Command |
|---|---|
| To configure change-log logging level.<br>Server related tasks and network related tasks are logged according to the task logging level. See Table 4-2.<br>The administrator configures the change-log so that all tasks with priority greater than or equal to the level configured will be logged. | `[SVR:/server](config)# change-log level {1-10}` |
| To view the change-log.<br>The change-log tasks can be filtered based on the username option or the number of tasks performed. | `[SVR:/server]# show change-log {user-name} { last <1-100000> }` |
| To clear the change-log.<br>This will clear all change-log entries or entries older than a specified number of hours or days. | `[SVR:/server]# clear change-log [older-than { days <1-240> \| hours <1-240> } ]` |

CHAPTER 5

# Managing Files

This chapter includes the following information:



## Saving a File

Cisco E-DI provides a way to save a command output to a file. Enter the following command to save a file:

```
[NET:/network]# show interfaces | save /server/interfacelist.txt
```

The file will be saved to the `/server` directory.

**Note** Scripts cannot be saved to the **/** directory of the server file system, or to the network file system.

CHAPTER 6

# Configuring Devices

Cisco E-DI supports configuration of devices, through the CLI, the GUI, and the XML programmatic interface (PI), covering a range of platform/OS combinations. Cisco E-DI uses a knowledge base which emulates each device to provide you with a virtual experience of configuring the actual device.

The knowledge base for the various platforms is learnt through the **FastTrack** command learning engine. Through FastTrack, Cisco E-DI is capable of providing comprehensive coverage for a given NE/OS release combination within a short period of time.

As more features are added into releases of Cisco IOS, Cisco E-DI incrementally builds upon the existing knowledge base through incremental device updates (IDU) that are available for download.The IDU feature allows Cisco E-DI to be updated with new device packages on the running system.

Cisco E-DI users can configure a group of devices using **network virtualization**. Cisco E-DI groups the knowledge base data applicable to all the devices in the group, and provides the common set of configuration commands to the user. In this way, the user can configure the network as if they are configuring a single device. See Network Virtualization, page 1-8 for details.

This chapter includes the following information:



# Using the CLI

All network related configurations through the CLI are performed in the server configuration setup command mode. This mode contains commands for entering into configuration mode for selected devices or combinations of devices to save, commit, schedule or discard configuration changes.

To configure a device or devices:

**Step 1** Select the device using the **network <device>** or **network <group>** commands, or by changing into the device directory using the **cd** command.

Enter the config-setup mode, enter **config s**.

**Note** The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

**Step 2** Enter **config t** to start editing the configuration.

**Step 3** When you have finished editing the configuration, exit the config mode.

**Step 4** You enter the config-setup mode where you can commit, discard or schedule the configuration change you have just made.

This chapter includes the following information:

- Configuring a Device Using the CLI
- Managing Configuration Files Using the CLI

# Configuring a Device Using the CLI

Cisco E-DI provides several ways to change the configuration of a device:

- Interactive configuration
- Changing the configuration through **copy** command

**Note** The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

Table 6-1 gives the commands available to enter the network configuration mode and configure the devices.

***Table 6-1 Commands to Configure Devices***

| Action | Command |
|---|---|
| To enter network configuration setup mode.<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | [NET:/network]# **configure setup** |
| To enter network configuration mode. | [NET:/network](config-setup)# **conf t** |
| To enter the device configuration mode. | [NET:/network](config-setup)# **configure** [device \| terminal] ip-address |
| To exit from the current configuration view and move to the parent view. | [NET:/network](configure)# **exit** |
| To exit out of the configuration mode.<br>You can also use Ctrl-Z. | [NET:/network](configure)# **end** |

*Table 6-1 Commands to Configure Devices (continued)*

| Action | Command |
|---|---|
| To configure an interface when only one device is selected. | `[NET:/network](configure)# interface FastEthernet0/1` |
| To configure an interface when multiple devices are selected. | `[NET:/network](configure)# interface ip-address/name` |
| To configure an interface using an interface macro to select multiple interfaces.<br>Enter **interface ?** to see list of all macros available.<br>Devices can be grouped as interface macros. For example all-fast ethernet or all-VLANs.<br>This allows you to apply the configuration to all interfaces of the device, and also on all the devices in the selected group. | `[NET:/network](configure)# interface all-dot11` |
| To show the list of devices selected for configuration, or to preview the configurations that will be made on the selected device. | `[NET:/network](config-setup)# show [devices \| preview]` |
| To:<br>• Discard the configuration.<br>• Save the configuration as text and script to a file. The script will be saved in the /server/scripts/config-jobs directory.<br>• Schedule the configuration commit to a later date. The script will be saved in the /server/scripts/config-jobs directory.<br>• Commit the configurations to the devices immediately. Maintains a transaction log in /server/logs/config-commit.log and in user log file if user specifies. | `[NET:/network](config-setup)# discard \| save \| schedule-job \| commit [logfile FILENAME]` |
| To run the script. | `[NET:/network]# run file Script_path` |

In network configuration mode, Cisco E-DI provides a common set of commands that apply to all selected devices and their software versions.

After exiting from network configuration mode, you must select an option from the Configuration menu as follows:

## Validating Commands

Once the devices are selected for configuration, a summary table shows which devices have been selected and which versions of the knowledge base are being used to perform CLI operations.

In the network-config mode, enter CTRL-G to display the devices selected, knowledge base applied and the applicability of the command to the selected device. For example:

```
[NET:/network](configure)# ip name-server [CTRL-G]
Device            IDU Name    IDU Version   Version       Command Status
172.168.3.22      Cat3550     1.2           12.3(6a)      INCOMPLETE
172.168.3.21      Cisco7200   1.1           12.3(6a)      INCOMPLETE
```

# Managing Configuration Files Using the CLI

Cisco E-DI archives start-up and running-config files for all devices and the server whenever there is a configuration change.

You can use the archived files later to restore the configuration of the network or server to the desired state. All the network and server configuration archives are stored in the /server/config-archive directory.

Table 6-2 gives the commands to manage the configuration files.

***Table 6-2 Commands to Manage Configuration Files***

| Action | Command |
|---|---|
| To list all archives of running configuration.<br>A running configuration can be saved to the startup configuration.<br>The archived configuration files can also be viewed in the device directory, enter:<br>**cd /network/device/<ip address>/[running-config \| startup-config]** | [SVR:/server]# **show running-config** [archive \| device \| diff-with \| list-archives] |
| To list all archives of startup configuration | [SVR:/server]# **show startup-config** [archive \| device \| diff-with \| list-archives] |
| To load the latest archived configuration into the running configuration, or load the filename that points to the startup configuration.<br>The filename is the name of the startup configuration file to be loaded. | [SVR:/server]# **load-config** [*filename*] |
| To clear the configuration archive files from the server.<br>See Table B-1 for details of the options available with this command. | [SVR:/server]# **clear config-archive** [all \| device \|running-config\| startup-config] |
| To clear the configuration archive files from the network.<br>This command is applied to all the devices in the current context; **all** clears the startup and running configurations, **running** clears the running configurations, **startup** clears the startup configurations | [NET:/network]# **clear config-archive** {all \| startup \| running} |
| To clear the configuration archive files for a particular device. | [NET:/network]# **clear config-archive** device ip-address {all \| startup \| running} |
| To clear the configuration archive older than a specific period. | [NET:/network]# **clear config-archive** {**all** \| **running** \| **startup** \| **device** {**ip-address**} ...} **older-than** {**days** \| **time**} |

*Table 6-2 Commands to Manage Configuration Files (continued)*

| Action | Command |
|---|---|
| To restore a server or a device or a group of devices to a state represented by a specified time or a configuration file or a labeled archive file.<br>`file` is the name of the configuration archive file that will be used for restoration.<br>`time` restores the configuration file that has a timestamp that is less than or equal to the given time.<br>**Note** The device will be restarted after a configuration restore. | `[SVR:/server\|NET:/network]# restore {file file_name \| time YYYY MM DD HH:MM:SS \| label label_name}` |
| To create a label for server configuration.<br>Startup configuration archive files can be labeled using the time stamp or filename. Labels created in one context, for example server, are not displayed in the other context, that is network mode.<br>The label command accepts the name of the label and applies the label based on whether the command is implemented in the server or network context. | `[SVR:/server]# label {label_name} [descr \| file \| time]` |
| To create a label for device configuration.<br>`descr` provides an option to specify a description while labeling the configuration<br>`file` applies the label to the given file name.<br>`time` creates and applies a label based on the timestamp of the configuration archive file. | `[SVR:/server]# network [ip-address \| group {group-name} ]`<br>`[NET:/network]# label {label_name} [descr \| file \| time]` |
| To display the label and its details including the associated file, and description. | `[SVR:/server\|NET:/network]# show labels [detail label_name]` |
| To delete a label. | `[SVR:/server]# clear label server_conf \| network_conf {time YYYY MM DD HH:MM:SS descr "Server configuration as of <date> \| file_name descr "name"}` |

# Configuring Devices Using the GUI

The Cisco E-DI provides Device Configuration Manager (DCM), an Eclipse-based GUI application to view and edit a configuration before applying the changes to the device. DCM includes Command Editor.

DCM can be used to edit the contents of the startup configuration file and the running configuration file, and apply the configuration to the device.

DCM is packaged with Cisco E-DI, and will be available after you have installed Cisco E-DI. To install Cisco E-DI, see:

- *Installation Guide and Setup Guide for Enhanced Device Interface, 2.2 on Windows*
- *Installation Guide and Setup Guide for Enhanced Device Interface, 2.2 on Linux*

See these topics:

- Launching Device Configuration Manager (DCM) to launch DCM.
- Editing a Configuration File Using the DCM GUI for the procedure on editing a configuration file.
- Using the DCM Command Editor to Enter Commands and Check Command Syntax to check your command syntax using DCM.

# Launching Device Configuration Manager (DCM)

Before you launch Device Configuration Manager, from the command prompt, navigate to your Eclipse folder (where eclipse.exe resides). Run the command `eclipse -clean`

This ensures that the cache is cleaned.

After you have installed Cisco E-DI, follow these steps to launch DCM.

**Note** Before you start DCM, ensure that the EDI Service is running. To start this service, go to **Start > Programs > Cisco E-DI > E-DI Service > Start**.

After you have installed Cisco E-DI, follow these steps to launch DCM. DCM is a client application that can be used to connect to any E-DI server. It is recommended that you use Windows client with a Linux server.

Before you start DCM, ensure that the EDI Service is running.
To start this service, On Windows, go to **Start > Programs > Cisco E-DI > E-DI Service > Start**.
On Linux, navigate to *E-DI Install Location* /Cisco-EDI/bin and enter `./start` at the command prompt.

**Step 1** On Windows:

- Choose **Start > Programs > Cisco E-DI > E-DI Service > Device Configuration Manager**. The Device Configuration Manager perspective opens.

or

- Navigate to the directory *E-DI Install Location*\Cisco EDI\edi\dist\ui_products\configmanager and double-click on **launcher .exe**.

On Linux:

- Navigate to *E-DI Install Location*/Cisco EDI/edi/dist/ui_products/configmanager and enter `./launcher`

**Step 2** E-DI prompts you to log in to the E-DI server.

**Step 3** Log in using the admin credentials.

Select the SSH check box if you want to run DCM in SSH mode.

By default, DCM connects to the port 2323 on the server

If the server Telnet port is not 2323, you should change this value in the **eclipse.ini** file. This file is located in the following location:

On Windows:

*E-DI Install Location*\edi\dist\ui_products\configmanager.

On Linux:

*E-DI Install Location*/edi/dist/ui_products/configmanager

After you log in, Device Configuration Manager opens. This has three perspectives (which appear as buttons):

- Config Manager—This is the default perspective, and this button is highlighted. See Figure 6-1.
- Macro Command Manager—Opens the Macro Command Manager perspective.See Figure 6-1.
- Command Translator—Opens the Command Translator perspective. To display the Command Translator button, click on the >> symbol that appears after the Macro Command Manager Button. See Figure 6-1. After you click on >>, the Command Translator button appears. See Figure 6-1

***Figure 6-1 Device Configuration Manager default perspectives and the >> symbol***

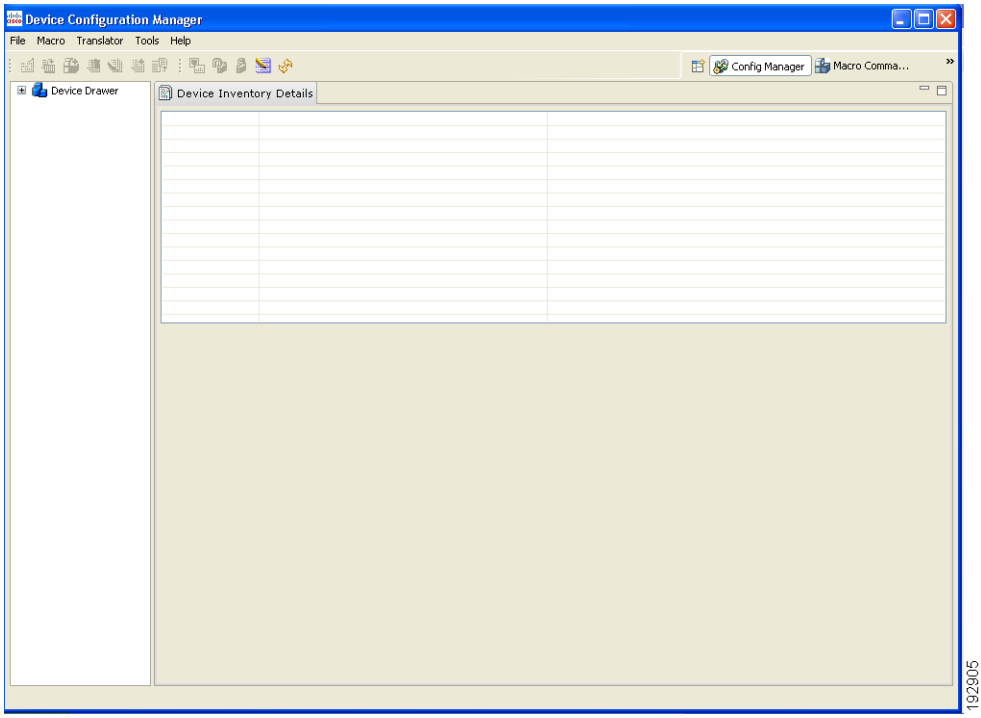
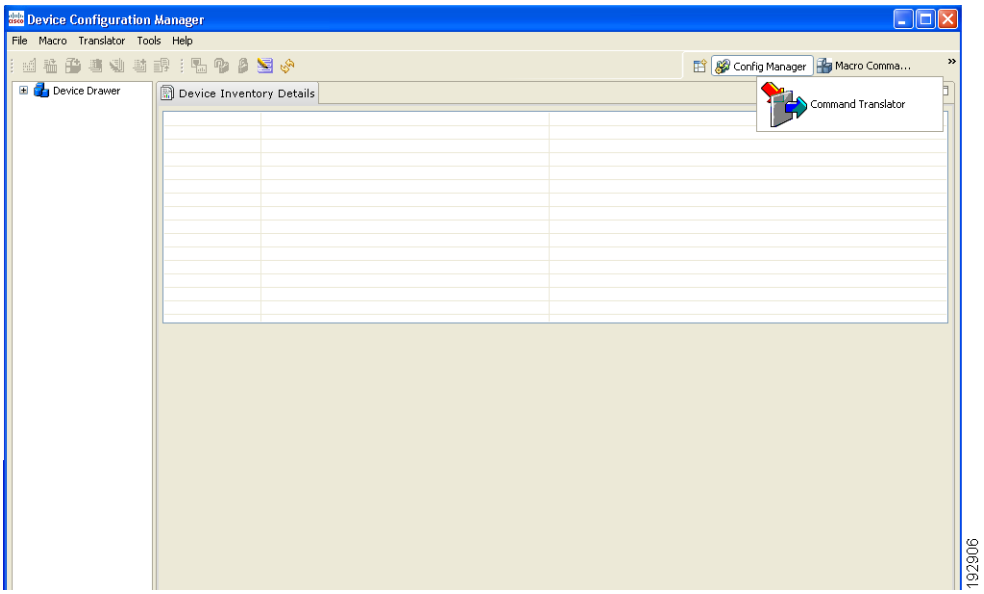


*Figure 6-2 The Command Translator button appears*




For a description of the DCM views, see Understanding the DCM UI.

Right-click on a device. The context menu that appears displays the options Edit Running Config, Edit Startup Config etc.

For the complete procedure on editing configuration files using DCM, see Editing a Configuration File Using the DCM GUI.

# Understanding the DCM UI

The DCM perspective is divided into these main sections:

- Tree View

  Displays the network folder (Device Drawer). After you log into the E-DI server, you can expand the Network folder to view all your managed devices in this pane.

  You can right-click on the Device Drawer and select Refresh Network from the context menu to view any newly managed devices in the Device Drawer.

- Device Inventory View

  When you first open Device Configuration Manager, expand the device drawer and select a device, the device inventory details appear in the Editor area.

  These details include IP Address, Name, Vendor name, OS Name, OS version, Managed Status, Online Status, Device Type, Device Family, System Description, and System OID.

- Editor Area

  Displays the startup and running config files that you have opened, and also the Command Editor. The tabs in this view allow you to navigate between the various open files and the Command Editor.

DCM allows you to save the editing contents to a file on a user local file system for viewing later. When you open a file from the user local file system, it opens in the Editor area of DCM.

The tab header displays a text icon and *devicename*_running or *devicename*_startup. You can open multiple files and they appear in the Editor area with appropriate tab headers.

For the complete details about editing configuration files, see Editing a Configuration File Using the DCM GUI.

The Command Editor (**Tools > Command Editor**) can be used to edit the contents of running configuration file. The changes are saved to a file. The changes cannot be applied directly to the device from the Command Editor.

You can also change device type and IOS version for checking command syntax. The command syntax check will be done based on the device knowledge base.

# Editing a Configuration File Using the DCM GUI

You can use Device Configuration Manager (DCM) to edit a running configuration file or a startup configuration file.

To use DCM for edits:

**Step 1** Launch DCM (see Launching Device Configuration Manager (DCM)).

**Step 2** From the Device Drawer in the Tree View, select a device.

An asterisk (*) indicates that the device is not supported in Cisco E-DI. The Device Inventory view displays the device properties of the selected device.

**Note** Access to edit a device configuration is only available to a user with full control access including permission to change that device configuration.

**Step 3** Edit the configuration file as required.

The editing options are:

- To edit a running configuration, right-click on the device in the Device Drawer, and select **Edit Running Config** from the context menu that appears.

  A copy of the running configuration appears in the Editor area (right central view). You can edit this copy. A tab identifies the running configuration.

- To edit a startup configuration, right-click on the device and select **Edit Startup Config** from the context menu that appears.

  A copy of the startup configuration appears in the Editor area (right central view). You can edit this copy. A tab identifies the startup configuration.

From the Edit option on Eclipse Menu Bar, or from context-menu that appears when you right-click in the Editor, you can use Cut, Copy, Paste, Undo, Redo, and other Edit options to make your edits.

You can lock the file so that other users cannot make changes to the device.

To lock or unlock a device:

- Select the device and then select **Tools > Lock Device** from the Eclipse Menu Bar.
- Select **Tools > Unlock Device** from the Eclipse Menu Bar to unlock the file. You can also select a device and right-click. A context menu appears. You can use the Lock Device/Unlock Device Options from here.

You can search for a word or phrase, using **Edit > Find/Replace** from the Main Menu Bar.

The Editor includes the option to check the command syntax based on the knowledge base for that device. The CLI syntax is checked automatically as you make your edits to the running or startup config.

The content text in the Editor area is color coded to give visual feedback as follows:

*Table 6-3 Syntax Colors*

| Command Text | Color | Font Type | Example |
|---|---|---|---|
| Known command keywords | Dark Blue | Bold | **interface** |
| Incomplete command keywords | Black | Italic | *interf* |
| Valid parameter words | Green | Normal | FastEthernet0/0 |
| Unknown command keywords | Red | Normal | itnerface |
| Comments | Grey | Normal | ! comments |

The CLI syntax is also checked automatically within your open file when you choose a different Device Family and Version. The comments will be shown in a different syntax color and font as syntax checking feedback.

This is a tool for checking whether one configuration file can be applied to another device family. It can also be used as a training or learning aid, or to compare commands.

The device details and version are shown in the Status bar. A different color is used to distinguish submode blocks, for example **username** cisco **password 0** cisco.

If you enter **Ctrl <Space>**, E-DI displays hints on the commands and parameters. These will help you in entering the commands correctly.

**Step 4** From the Eclipse Menu Bar, click **Apply To > Running Config** to apply the changes to the running configuration file. If you try to make further changes to the file before the device is synchronized with the updated file, you will see an error message.

To close the Editor, choose the cross sign on the tab. If you had made any changes, you will be asked to save your changes.

# Using the DCM Command Editor to Enter Commands and Check Command Syntax

You can use the DCM Command Editor to create command sets and check any command syntax against a device family and OS version:

**Step 1** Launch DCM. See Launching Device Configuration Manager (DCM) for details.

**Step 2** From within the DCM perspective, select a device from within the Network folder.

**Step 3** From the Main Menu Bar, select **Tools > Command Editor**.

The Command Editor opens.

**Step 4** Enter the command, and choose the device family and OS version from the drop down lists in the top view.

As you enter commands, the DCM syntax checker checks for your syntax. The color codes provide you with visual feedback.

**Step 5** Save the command to a file.

This file can be reopened in the Command Editor to check against the required the device family and OS version (selected from the top right view).

You can modify the content and verify the syntax.

You can open the running configuration file for the device using the Device Configuration Manager.You can copy commands from the Command Editor to the Device Configuration Manager to apply the translated commands to the device configuration.

# Viewing Device Interfaces

You can view the details of all the interfaces on a particular device.

**Step 1** Right-click on a device in the Device Drawer.

**Step 2** Select **Show Interface** from the context menu that appears.

The Interface List appears.

The Interface List pop-up appears, displaying the following information:

| Fields | Description |
|---|---|
| Device IP | IP address of the device |
| Interface Name | Name of the interface. For example, FastEthernet0/1 |
| Interface Type | Type of the interface. For example, Loopback. |
| Physical Address | MAC address. |
| IP Address | Interface IP Address. |
| Network Mask | Network mask of the interface. |
| Admin Status | Administrative Status (up or down). |
| Oper. Status | Operational Status (up or down). |

CHAPTER 7

# Managing Inventories and Reports

Cisco E-DI maintains an inventory of the devices that are in its management domain. This information is used for configuring the network through the XML Programmable Interface and the CLI.

Cisco E-DI also collects Layer 2 data reports which can be used when diagnosing Layer 2 connectivity issues in the network.

This chapter includes the following information:



## Inventory Information

For each device, Cisco E-DI initially collects the following physical inventory information from the NE interface through the SNMP protocol:

- Device type
- OS version
- List of interfaces/status through IF-MIB
- List of modules/slots/ports through ENTITY MIB if supported by the device/OS version

Inventory information can be collected manually in network mode.

Cisco E-DI collects inventory automatically on a periodic basis, however a manual inventory can be triggered at any time using the **inventory** command.

A typical inventory can collect the following performance statistics:

- Interface performance—This inventory collects interface performance statistics including errors, packet discards and actual throughput. The report reflects changes between the last poll cycle and the current one.
- Device performance and resources —This inventory collects all device performance and resources parameters, for example CPU utilization, and memory utilization.

Cisco E-DI collects the following inventory data. Inventory collection for each category can be done independently:

- Basic inventory:
  - Device basic data
  - Device interface data

  - Device status polling
- Extended inventory
  - Device file system information
  - Device asset information
  - Device configuration information
- Performance and miscellaneous inventory
  - Device CPU utilization
  - Device interface status
- Application inventory
  - Device ARP, CAM, STP, VTP data

Each category of inventory data is collected through one or more configurable services. Each inventory service polls the device at regular intervals to collect or synchronize data. The following services can be configured independently depending on the user's requirements, and to improve performance:

- Basic inventory and status-polling—This is a mandatory service and cannot be turned off
- File system—Disabled by default
- Configuration file manager—Enabled by default
- Asset—Disabled by default
- Performance—Disabled by default
- ARP table—Disabled by default
- VTP—Disabled by default
- STP—Disabled by default

The results of each inventory collection service can be displayed.

Cisco E-DI also includes a service that the administrator can use to manage the assets in the network. The service provides details of the hardware and the associated information for each of the device in the network. For example chassis, cards, ports, fans, and power supply.

Using the asset inventory management service, an administrator can view:

- All the hardware assets contained in the device including the name, type and identifier of each of the asset. This enables tracking of individual assets on the devices.
- Chassis information of each device, for example, the serial number, hardware revision, and a brief description of the chassis. This provides details of the hardware information of the chassis without requiring a physical inspection of the device.
- Information on the cards and modules available in the device including the name and identifier of the card, and the container that holds the card. This tracks the cards, and their position in the device.
- Slot information in the device, for example the number of chassis slots, cards contained in the slot, slots that are empty, and daughter card slots.
- Port information in the device which gives the list of ports on the device and the location of each port.
- Power supply information in the device. There can be one or more power supply modules in a device. The report gives information about the number of these modules, and also the wattage of each power supply module.
- Fans in each device.

Cisco E-DI collects an inventory of the assets at regular intervals. However, you can do a manual inventory to synchronize the updated asset information with Cisco E-DI, see Table 7-2.

# Manual Inventory

To perform an inventory on a device in the current context, enter the following command:

```
[NET:/network]# inventory
```

**Note** The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

# Configuring the Inventory Service

You can configure services in Cisco E-DI according to the category of inventory data required, see Table 7-2 for commands.

***Table 7-1 Commands to Collect Inventory Data***

| Description | Command |
|---|---|
| To enable the status poller service.<br>You can view the current frequency of any task, enter **show job details** *<task-name>*. | [SRV:/server](config)# **service statuspoller** |
| To set the polling frequency of the status poller service.<br>You can view the current frequency, enter **show job details** *<task-name>*. | [SRV:/server](conf-statuspoller)# **poll-interval** <poll-frequency> |
| To enable the inventory service.<br>You cannot disable the inventory service. | [SRV:/server](config)# **service inventory** |
| To set the polling fequency of the inventory service.<br>You can view the current frequency, enter **show job details** *<task-name>*. | [SRV:/server](conf-inventory)# **poll-interval** <poll-frequency> |
| To enable the performance service. | [SRV:/server](config)# [**no**] **service performance** |
| To set the polling frequency of the performance service.<br>You can view the current frequency, enter **show job details** *<task-name>*. | [SRV:/server](conf-performance)# **poll-interval** <poll-frequency> |
| To enable the configuration service.<br>You cannot set the frequency for the configuration service. The configuration collection is driven by Syslog messages received by Cisco E-DI and the inventory service.<br>Every inventory collection triggers a configuration collection. That means that the frequency of the configuration collection service is the same as the frequency set for the inventory service. | [SRV:/server](config)# [**no**] **service config** |

*Table 7-1 Commands to Collect Inventory Data (continued)*

| Description | Command |
|---|---|
| To enable the file system service.<br><br>You cannot set the frequency for the file system service. The file system collection is driven by Syslog messages received by Cisco E-DI and the inventory service.<br><br>Every inventory collection triggers a file system collection. That means that the frequency of the file system collection service is the same as the frequency set for the inventory service.<br><br>**Note** If the filesystem service is disabled, the **dir** command under the device context shows the following warning message, Warning: filesystem service is disabled. Enter **sync filesystem fg** to manually synchronize the data. | `[SRV:/server](config)# [no] service filesystem` |
| To display the configuration of the services to collect inventory data. | `[SRV:/server]# show running-config` |

# Viewing the Inventory

You can view the inventory report, see Table 7-2 for commands.

*Table 7-2 Commands to View the Inventory*

| Description | Command |
|---|---|
| To show the data collection status for a device. Data may be collected by a system triggered task (by the poller) or by a user initiated task (**inventory**, **sync asset**, **sync config** and **sync file system**).<br>Example output:<br>`Device Inventory StartTime EndTime Status Message Type`<br>`172.16.0.0 Perf 09/05/2005 11:19 09/05/2005 11:19 Finished Success`<br>`172.16.0.0 Asset 09/05/2005 11:19 09/05/2005 11:19 Finished Success`<br>`172.16.0.0 Config 09/05/2005 11:19 In-Progress`<br>`172.16.0.0 Perf 09/05/2005 11:18 09/05/2005 11:18 Failed Failed for Spec If-Performance-Inventory`<br>`172.16.0.0 Asset 09/05/2005 11:18 09/05/2005 11:18 Finished Success`<br>`172.16.0.0 Config 09/05/2005 11:18 In-Progress`<br>Inventory type:<br>• Perf—Performance data<br>• Asset—Asset data<br>• Config—Configuration data<br>• FileSystem—Devices file system information<br>The Message column shows whether a task has completed successfully or failed.<br>If the task is running at the time of report, the Status column shows In-Progress. | `[SRV:/server]# show status inventory` |
| To view all the assets of all the devices in the network.<br>A warning message is displayed if this device is disabled. Enter **sync asset fg** to manually synchronize the data. | `[NET:/network]# show asset all` |
| To view the chassis information including serial number, hardware revision.<br>A warning message is displayed if this device is disabled. Enter **sync asset fg** to manually synchronize the data. | `[NET:/network]# show asset chassis` |
| To view the cards available on each device including the those that are on the chassis slots and also on the other cards.<br>A warning message is displayed if this device is disabled. Enter **sync asset fg** to manually synchronize the data. | `[NET:/network]# show asset cards` |

*Table 7-2 Commands to View the Inventory (continued)*

| Description | Command |
|---|---|
| To view the slots that are available in the chassis of the device and also on the daughter card modules.<br>A warning message is displayed if this device is disabled. Enter **sync asset fg** to manually synchronize the data. | [NET:/network]# **show asset slots** |
| To view the ports that are available on a device.<br>A warning message is displayed if this device is disabled. Enter **sync asset fg** to manually synchronize the data. | [NET:/network]# **show asset ports** |
| To view the power supply available on the device.<br>A warning message is displayed if this device is disabled. Enter **sync asset fg** to manually synchronize the data. | [NET:/network]# **show asset power-supply** |
| To view the fans present on a device.<br>A warning message is displayed if this device is disabled. Enter **sync asset fg** to manually synchronize the data. | [NET:/network]# **show asset fans** |
| To synchronize the updated asset information with Cisco E-DI. Synchronization can be done in the foreground or the background. | [NET:/network]# **sync asset** {**bg** \| **fg**} |
| To show cdp information for managed devices. | [NET:/network]# **show cdp neighbors** |
| To list all interfaces in the current network view. | [NET:/network]# **show interfaces** |
| To show IP information. | [NET:/network]# **show ip interface brief** |
| To show a report on the alarm state of the device over a period of time. | [NET:/network]# **show report availability** |
| To show detailed cpu-utilization information on the device over a period of 5 minutes.<br>A warning message is displayed if this performance service is disabled. The data may not be up-to-date. | [NET:/network]# **show report cpu-utilization** |
| To display a list of all devices in the current context. | [NET:/network]# **show report device-list** |
| To show a report on the alarm state of the device over a period of time.<br>A warning message is displayed if this performance service is disabled. The data may not be up-to-date. | [NET:/network]# **show report if-performance-summary** |
| To show the interface utilization.<br>A warning message is displayed if this performance service is disabled. The data may not be up-to-date. | [NET:/network]# **show report if-utilization-summary** |
| To show the current software version on all the devices. | [NET:/network]# **show report software** |
| To display the network running configuration.<br>See Table B-1 for details of the options available with this command. | [NET:/network]# **show running-config** |
| To display the network startup configuration.<br>See Table B-1 for details of the options available with this command. | [NET:/network]# **show start-up-config** |
| To show the software version. | [NET:/network]# **show version** |

The asset inventory service can be enabled or disabled in Cisco E-DI. See Table 7-3.

*Table 7-3 Commands to Enable or Disable the Asset Inventory Service*

| Action | Command |
|---|---|
| To navigate to the server configure mode. | `[SRV:/server]# configure terminal`<br>or<br>`[SRV:/server]# config t` |
| To enable the asset management service. | `[SRV:/server](config)# service asset` |
| To disable the asset management service. | `[SRV:/server](config)# no service asset` |

# Layer 2 Information

Cisco E-DI collects the following Layer 2 information through the SNMP protocol and Telnet for each device for which the information is available, and provides reports which can be used when debugging Layer 2 connectivity issues in the network:

- ARP data—Address Resolution Protocol. The Internet protocol used to map an IP address to a MAC address. Supported on all Cisco IOS, CATOS and PIX devices.
- MAC(CAM) table data—Media Access Control. Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures.
- VLAN/VTP data
  - Virtual LAN—Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.
  - VTP data—Virtual Terminal Protocol. ISO application for establishing a virtual terminal connection across a network.
- STP data—Spanning-Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree.

The L2 data collection is disabled by default when the Cisco E-DI server starts. The service must be enabled to start collecting the data. The System Administrator can enable or disable data collection using the service commands in the Cisco E-DI configuration mode.

Layer 2 data collection is supported on CATOS and Cisco IOS devices that support the Bridge.Mib and Cisco-VTP-mib.

The Layer 2 data reports collected from the devices are archived into the database. When the database reaches one million events, the oldest 10% of events are discarded.

There are two methods to synchronize the data reports on Cisco E-DI with the devices:

- Specify the polling option in the configuration mode
- Manually synchronize Cisco E-DI with the devices

**Note** If frequent polling is specified, this can have an adverse effect on performance.

# Collecting ARP Data

ARP information from all the devices can be collected periodically and maintained in the database. The report includes protocol, age of entry, MAC address of the device, and the interface the entry was learnt on. See Table 7-4 for the commands.

*Table 7-4 Commands to Collect ARP Data*

| Description | Command |
|---|---|
| To change to configuration mode. | `[SVR:/server]# config t`<br>`[SVR:/server] (config)#` |
| To disable the ARP service. | [SRV:/server](config)# **no service arp** |
| To enable the ARP service.<br>To enter the config-arp sub mode. | [SRV:/server](config)# **service arp** |
| To configure the frequency of polling in minutes. | [SRV:/server](config-arp)# **poll-interval** *<5-1000>* |
| To manually synchronize the local ARP information with that of the device in the current context. | `[NET:/network]#` **sync arp** |

*Table 7-5 Commands to View ARP Data Records*

| Description | Command |
|---|---|
| To view all the ARP entries on the devices in the network | `[NET:/network]#` **show arp** |
| To view all ARP entries for the specified ip address | `[NET:/network]#` **show arp ipaddress <A.B.C.D>** |
| To view all ARP entries for the specified mac address | `[NET:/network]#` **show arp macaddress <H.H.H>** |

Sample ARP data report:

```
Age   -   Age (Minutes)

 Device         Protocol Address        Age Hardware Addr   Type Interface
 --------------- -------- --------------- --- -------------- ----
 172.25.86.109   Internet 172.25.86.5      0 00c0.9f61.7b61 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.1      1 0009.e831.d8ff ARPA Vlan205
 172.25.86.109   Internet 172.25.86.42   113 00e0.812d.0a9f ARPA Vlan205
 172.25.86.109   Internet 172.25.86.76     3 0012.3f24.e706 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.77     0 0004.235f.4235 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.78     5 0004.23a7.85d1 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.72     0 0004.23a6.3759 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.73     0 0004.23a6.7247 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.74     2 00c0.9f3f.2e2f ARPA Vlan205
 172.25.86.109   Internet 172.25.86.71     0 0002.55b7.6fa3 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.109    - 0008.e3c3.6b00 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.140   21 0040.9655.c861 ARPA Vlan205
 172.25.86.109   Internet 172.25.86.141    7 0012.da3e.5348 ARPA Vlan205
```

# Collecting MAC Address Table Information

MAC address table information from all the devices that report such information can be collected periodically and maintained in the database.

The report includes the VLAN, the port the entry was learned on, MAC address, and VLAN type. Filters can be set up to filter by MAC address or VLAN or VLAN type. See Table 7-6 for the commands.

***Table 7-6 Commands to Collect MAC Address Table Entries***

| Description | Command |
|---|---|
| To change to configuration mode. | `[SVR:/server]# config t`<br>`[SVR:/server] (config)#` |
| To disable the MAC address table service. | `[SRV:/server](config)# no service mac-address-table` |
| To enable the MAC address table service.<br>To enter the config-mac-address-table sub mode. | `[SRV:/server](config)# service mac-address-table` |
| To configure the polling frequency in minutes. | [SRV:/server](config-mac-address-table)# **poll-interval** *<5-1000>* |
| To synchronize the local MAC address table information with that of the device in the current context. | [NET:/network]# **sync mac-address-table** |

***Table 7-7 Commands to View MAC Address Table Entries Records***

| Description | Command |
|---|---|
| To view all the CAM entries on the switches in the network. | `[NET:/network]# show mac-address-table` |
| To view all the CAM entries on the switches in the network which match with the specified mac address. | `[NET:/network]# show mac-address-table address <H.H.H>` |
| To view all the dynamic CAM entries on the switches in the network. | `[NET:/network]# show mac-address-table dynamic` |

*Table 7-7 Commands to View MAC Address Table Entries Records (continued)*

| Description | Command |
|---|---|
| To view all the static CAM entries on the switches in the network. | `[NET:/network]# show mac-address-table static` |
| To view all the CAM entries for specified vlan on the switches in the network. | `[NET:/network]# show mac-address-table vlan <vlan_id>` |

Sample MAC address table report:

```
admin@edi-jms-1[172.25.86.109 #show mac-address-table
 Switch Address   Address          Type             VLAN Port
------------------------------------------------------------
 172.25.86.109   00c0.9f61.7b61  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0014.f21f.9370  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0014.6969.57a8  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0013.8028.1c04  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0012.da3e.6fff  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0012.d923.a306  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0011.20db.88d2  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   000b.4556.73ff  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0009.e831.d8ff  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0009.7b9e.317c  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0008.e3db.df3e  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0007.8508.554a  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0007.0ea7.71aa  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0004.23a6.7247  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0004.23a6.3759  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0004.235f.4235  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0003.ba0f.cbc7  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0003.ba0f.a63f  DYNAMIC  205 FastEthernet0/1
 172.25.86.109   0002.55b7.6fa3  DYNAMIC  205 FastEthernet0/1
 172.25.86.109    0001.42b1.c100  DYNAMIC  205 FastEthernet0/1
```

# Collecting VLAN and VTP Data

VLAN and VTP status and statistics information from all the devices that support VTP can be collected periodically and maintained in the database. The report includes the mode, version and revision of the VTP configuration database for all the devices in each domain.

VTP statistics reports also provide information on the number of VTP advertisements sent and received, and configuration revision/digest errors. See Table 7-8 for the commands.

The reports can include the following information:

- Status of VLAN in the entire network on a per-domain basis
- Status of the access and trunk ports
- VLAN mapping of ports
- Additional trunk port status including encapsulation

*Table 7-8 Commands to Collect VTP Data*

| Description | Command |
|---|---|
| To change to configuration mode. | `[SVR:/server]# config t`<br>`[SVR:/server] (config)#` |
| To disable VTP service. | `[SRV:/server](config)# no service vtp` |
| To enable VTP service.<br>To enter the config-vtp sub mode. | [SRV:/server](config)# **service vtp** |
| To configure the polling frequency in minutes. | [SRV:/server](config-vtp)# **poll-interval** *<5-1000>* |
| To synchronize the local VTP information with that of the device in the current context. | [NET:/network]# **sync vtp** |

*Table 7-9 Commands to View VLAN and VTP Data Reports*

| Description | Command |
|---|---|
| To view the VLAN status information including the domain, VLAN Id, VLAN name and the status of the VLAN. | `[NET:/network]# show vlan` |
| To view the status of both trunk and access ports of all the switches in the current context.<br>To view all the ports configured to function as access ports. | `[NET:/network]# show vlan ports` |
| To view the status of the trunk-ports with additional information like encapsulation.<br>To view all the ports configured to function as trunk ports. | `[NET:/network]# show vlan trunk-ports` |
| To view all the VTP trunking statistics. | `[NET:/network]# show vtp counters` |
| To view the VTP status information of all devices in the current context. | `[NET:/network]# show vtp status` |

Sample VTP status report:

```
Device Domain Mode Ver Rev Last Updater Pruning State
------------ ---------- --------- ---- --- ------------ ----------------- ---------------

172.25.86.108 Server 2 0 0.0.0.0 Disabled
172.25.86.106 Server 2 0 0.0.0.0 Disabled
172.25.86.104issc-2Transparent2 0 172.25.86.104 Disabled
172.25.86.103isscTransparent 2 0 172.25.86.103 Disabled
172.25.86.116 lab Server 2 20 172.25.86.116 Disabled
172.25.86.109issc-1 Transparent 2 0 0.0.0.0 Enabled
```

# Collecting STP Data

STP information on a per-VLAN basis can be collected periodically and maintained in the database. The report includes the STP status of the bridge including priority, number of ports, root port, cost and the state (blocked/forwarding/…) of the ports. See Table 7-11 for the commands.

*Table 7-10 Commands to Collect STP Data*

| Description | Command |
|---|---|
| To change to configuration mode. | `[SVR:/server]# config t`<br>`[SVR:/server] (config)#` |
| To disable STP service | [SRV:/server](config)# **no service span-tree** |
| To enable STP service. Also enter into config sub mode config-span-tree | [SRV:/server](config)# **service span-tree** |
| To Configure the frequency of polling in minutes. | [SRV:/server](config-span-tree)# **poll-interval <***5-1000***>** |
| To synchronize the local STP information with that of the device in the current context. | `[NET:/network]#` **sync span-tree** |
| To clear the local STP information. | `[NET:/network]#` **clear span-tree** |

*Table 7-11 Commands to View STP Data Reports*

| Description | Command |
|---|---|
| To view spanning tree information on a per-vlan basis for all the devices. | `[NET:/network]#` **show stp** |
| To view the spanning tree of the given vlanId. | `[NET:/network]#` **show stp vlan <vlanId>** |
| To show detailed bridge information for each port on the device such as port state (forwarding, disabled, etc.), cost, priority and vlan. | `[NET:/network]#` **show stp vlan <vlanId> port-state** |

Sample STP report:

```
* - STP designated Root

Device VLAN PriorityBridge ID Num RootRoot PortRoot BridgeCost
               of Ports   Priority
172.25.86.1031327690012.dae1.0080 11327680009.e830.6500   31
172.25.86.1032327700012.dae1.0080 10327700012.dae1.0080    0
172.25.86.103 205329730012.dae1.0080 21327680001.42b1.c101   42
172.25.86.116 132768000b.45f0.b800 6765327680009.e830.6500   42
172.25.86.116 632768000b.45f0.b800 2032768000b.45f0.b805    0
172.25.86.116 205000b.45f0.b8cc2650001.42b1.c101   69
172.25.86.116 805000b.45f0.b8cc20000b.45f0.bb24    0
```

CHAPTER 8

# Scheduling Jobs

Cisco E-DI provides the option to schedule EXEC mode and network configuration jobs. This is a useful tool for automating monitoring and operational tasks in a controlled fashion. A job can be scheduled for one time, or for repeated implementation.

Cisco E-DI keeps a history of jobs and logs. A scheduled job could be a Cisco E-DI command or a perl script. Typical tasks which could be scheduled would be the periodic synchronization of the Cisco E-DI data cache with the NE, or pushing configuration changes to NEs.

This chapter includes the following information:



## Scheduling EXEC Mode and Network Configuration Jobs

Table 8-1 gives the commands that you can use to schedule jobs.

*Table 8-1 Commands to Schedule Jobs*

| Action | Command |
|---|---|
| To create a job with a specified name. | `[SVR:/server](config)# schedule-job name` |
| To create a job with an optional description. | `[SVR:/server](config)# schedule-job name description Desc` |
| To define the commands to be run. Commands should be separated by semicolons (;) | `[SVR:/server](schedule-job)# execute cmd1; cmd2; ……` |
| To define the perl script to be run. | `[SVR:/server](schedule-job)# execute perl /users/admin/myperlscript.pl` |

*Table 8-1 Commands to Schedule Jobs (continued)*

| Action | Command |
|---|---|
| To specify when you want the job to start running.<br>The values are:<br>– Month—Name of the month<br>– Day—Day of the month<br>– Year—Between 2003-2020<br>– Hour—0-23<br>– Minutes— 0-59<br>**Note** You can modify any of the parameters of a scheduled job such as start time, stop time, and repeat frequency. Enter the command with the updated value. | `[SVR:/server](schedule-job)#` **`start-at month day year hour minutes`** |
| To specify when you want to the job to stop running. | `[SVR:/server](schedule-job)#` **`stop-at month day year hour minutes`** |
| To specify the repetition frequency with one of the frequency parameters listed above.<br>**Note** If you do not specify the repeat frequency, the job will be run once. | `[SVR:/server](schedule-job)#` **`repeat frequency [`***`minutes \| hours \| days \| weeks \|months \| years`***`] number`** |
| To delete a scheduled job. | `[SVR:/server](config)#` **`no schedule-job`** `name` |

The following example shows two scheduled jobs:

```
schedule-job Alarms
start-at april 7 2005 17 11
repeat frequency minutes 2
history-size 5
execute network ; clear alarms
!
schedule-job Inventory
start-at april 7 2005 17 10
repeat frequency minutes 2
history-size 5
execute network ; inventory
!
```

# Reviewing Scheduled Jobs

Table 8-2 provides options to review scheduled jobs, job implementation history, and detailed logs:

*Table 8-2 Commands to Review Jobs*

| Action | Command |
|---|---|
| To display a list of all jobs. | `[SVR:/server]# show job list` |
| To display details of the scheduled job. | `[SVR:/server]# show job details name` |
| To display all detailed logs of a job. | `[SVR:/server]# show job details name logs` |
| To display the latest job history. | `[SVR:/server]# show job details name logs latest` |

CHAPTER 9

# Handling and Reporting Alarms and Events

Cisco E-DI uses events received from devices, and data collected during polling and inventory, to maintain an accurate representation of the state of the devices and the network.

This data gives you an up-to-date view of the health of the device, and alerts you to configuration changes that are likely to fail. All events received from the network are automatically archived in the database. See Event Handling for more information.

Cisco E-DI also monitors certain events and performs automatic actions such as data synchronization and local status update. Any Cisco E-DI command or perl script can generate an event action.

When there are error conditions on the Network Elements, Cisco E-DI raises alarms and events as appropriate. The events are generated in standard Syslog message format so that external clients can subscribe to receive and process these events.

**Note** The timestamps for alarms and events use Cisco E-DI time, not the device time.

When the color mode is enabled, the Cisco E-DI CLI prompt indicates the NE's alarm aggregate status. The color of the prompt indicates the highest alarm severity found in the devices within the scope of the CLI mode. See CLI Color Mode, page 1-14 for more details.

When there are no alarms are on the device, the CLI prompt is white.

If session based device authentication is enabled, Cisco E-DI automatically sets the Syslog auto-subscription to Off. This means that you are notified that each managed device must be configured to forward the Syslog messages to Cisco E-DI either directly or through a Syslog relay agent.

You can configure one or more Syslog relays as valid Syslog generation sources. To do this, enter the configuration command **`relay-agent syslog`**.

Cisco E-DI automatically accepts messages from any pre-configured Syslog relay or directly from the NE. You do not have to choose one or the other.

This section includes the following information:

# Alarms

An alarm is a fault condition which needs attention from an administrator. Cisco E-DI monitors the network and itself to report network or server related alarms to the user. Alarms are raised based on the analysis of data obtained through polling of status and performance parameters, and the events received from the network.

The alarms are triggered according to user-defined conditions and thresholds, or by using default settings. Cisco E-DI captures the state of all NE interfaces, and represents them as NE alarms (if necessary). The NE's alarm aggregate status is indicated by the color of the CLI prompt.

Alarms can belong to either the server domain or the network. Basic parameters can be configured in the server configuration mode.

Alarms will be cleared automatically if the relevant network or server conditions are resolved. Alarms can also be cleared manually using the **clear alarms** command. See Table B-1 for details of the options available with this command.

All alarm related commands are context sensitive in the network and server domains.

All alarms are stored in the alarm history. Where Cisco E-DI is managing many devices, a large number of alarms is possible because of the number of interfaces and other components in the devices that potentially have associated states.

To avoid any performance issues, a limit is defined for the alarm history. This indicates how many entries each alarm will have in its history.

Table 9-1 describes the commands used to manage the alarm history data.

***Table 9-1 Commands to Manage the Alarm History***

| Action | Command |
|---|---|
| To define the size limit for the alarm history.<br>The default is 20 entries per alarm. | `[SRV:/server](config)# [no] alarm-history size <10-100>` |
| To configure the amount by which the alarm history is truncated.<br>Each time the number of alarms crosses the specified limit, the alarm history is truncated. The default value is 50%. | `[SRV:/server](config)# [no] alarm-history truncate <30-80>` |

# Alarm Parameters

Cisco E-DI alarms have the following parameters:

- Alarm condition—A network or server related qualitative or quantitative parameter that has a state or value, depending on which alarm is raised or cleared.
- State—Either **Active** or **Clear**.
- Default severity—Used when no thresholds are defined, or a pre-defined severity for an alarm has to be ignored.
- Alarm component—For a network, this is a sub-section of a device. For example, an interface or a module. For the server, it could be a module name.
- Alarm severity—A pre-defined state that signifies that level of severity. Alarms can be triggered with a specified severity based on a state value which can be Boolean or can be triggered with varying levels of severity based on the defined thresholds and the state value.

- Alarm thresholds—Specified by the you and associated to a condition value either as a percentage or a numerical value. Alarms that have thresholds can oscillate between different alarm severities according to the values associated to that condition.

# Alarm Conditions

The alarm conditions are given in Table 9-2.

***Table 9-2 Alarm Conditions***

| Alarm Condition | Unit | Threshold | Domain | Description |
|---|---|---|---|---|
| CPUOverloaded | % | Yes | Network | CPU utilization on the device is too high. |
| ConnectionFailed | No | No | Network | Failed to establish a Telnet/SSH connection to the device. |
| DBUnavailable | No | No | Server | Database connection unavailable on the server. |
| EDIDiskSpaceUsageHigh | | | | Cisco E-DI disk space usage is high |
| FCSErrors | % | Yes | Network | Too high FCSError rate (FCS errors vs. throughput) on a Radio interface. |
| FailedToLoad | No | No | Server | Server module failed to load. |
| HighMemPoolUtil | % | Yes | Network | High memory pool utilization on the device, expressed as used memory vs. total memory. |
| IfAdminDown | No | No | Network | Device interface administratively down. |
| IfDown | No | No | Network | Device interface operationally down. |
| IfOverloaded | % | Yes | Network | Interface utilization high, expressed as through-put vs. total-bandwidth. |
| IfPacketErrors | % | Yes | Network | Too high Packet error rate (packet errors vs. total throughput) on an interface. |
| LineProtoDown | No | No | Network | Interface line protocol down. |
| LoggingHostMismatch | No | No | Network | Logging settings on the device does not have Cisco E-DI as a Syslog event recipient. |
| MemAllocFailure | No | No | Network | Memory allocation failure on the device. |
| MemoryDefragmented | % | Yes | Network | Largest contiguous memory segment available vs. total available free space. |
| PrimaryServerUnavailable | | | | Primary server unavailable |
| RunningConfigUnavailable | No | No | Network | Running Config of the device is unavailable |
| SecondaryServerUnavailable | | | | Secondary server unavailable |
| StartupConfigUnavailable | No | No | Network | Startup Config of the device is unavailable |
| SwPolicyViolation | No | No | Network | Software on device does not conform to the policy specified. |
| TftpServerNotstarted | No | No | Server | TftpServer on the server failed to start. |
| TxFailedAfterMaxRetries | % | Yes | Network | Tx failures relative to through-put after allowed re-transmission attempts exceeded threshold. |
| Unreachable | No | No | Server | Device is not reachable using SNMP. |
| Unsupported | No | No | Network | Device not a recognized type. |

*Table 9-2 Alarm Conditions (continued)*

| Alarm Condition | Unit | Threshold | Domain | Description |
|---|---|---|---|---|
| VtpConfigDigestErrors | | | | VtpConfigDigestErrors |
| VTPConfigRevNumberErrors | | | | VTPConfigRevNumberErrors |

Table 9-3 gives the commands that you can use to display specific alarm conditions.

*Table 9-3 Commands to View Alarms*

| Action | Command |
|---|---|
| To show all alarms in active and cleared state. | `[NET:/network]# show alarms all` |
| To show alarms that match the given condition. | `[NET:/network]# show alarms condition condition-name` |
| To show the detailed history for the active alarms. | `[NET:/network]# show alarms details` |
| To show alarms that are of given severity. | `[NET:/network]# show alarms severity alarm-severity` |
| To show all alarms that match the given severity. | `[NET:/network]# show alarms all severity alarm-severity` |
| To show all alarms that match the given condition. | `[NET:/network]# show alarms all condition condition-name` |
| To show the details of all alarms in the network. | `[NET:/network]# show alarms all details` |
| To show active alarms that match the criteria specified in the filter. | `[NET:/network]# show alarms filter text` |
| To show all alarms that match the criteria specified in the filter. | `[NET:/network]# show alarms all filter text` |
| To show active alarms for the entire network. | `[NET:/network]# show alarms network` |
| To show active alarms for the server. | `[NET:/network]# show alarms server` |
| To show alarms for a device. | `[NET:/network]# show alarms device ip_address [all\| details \| [condition condition-name] \| [severity alarm-severity]]` |
| To show alarms for a group. | `[NET:/network]# show alarms group group-name [all \| details \| [condition condition-name] \| [severity alarm-severity]]` |
| To show alarms with a specified id. | `[NET:/network]# show alarms id number` |

# Configuring an Alarm Policy

To configure an alarm policy:

**Step 1** Login to the Cisco E-DI server with administrative privileges.

**Step 2** Enter into the configure mode:

```
[SVR:/server]# config terminal
```

**Step 3** Enter the following command to configure an alarm policy using the default alarm policy as a base:

```
[SVR:/server](config)# alarm-policy default
```

**Step 4** Enter the following command to configure an alarm condition, for example CPUOverloaded:

```
[SVR:/server](conf-alarm-policy)# define alarm-condition CPUOverloaded
```

**Step 5** Enter the following command to define the number of cycles to observe before the alarm is raised, for example 2:

```
[SVR:/server](def-cond-param)# cycles 2
```

**Step 6** Enter the following command to define the severity and threshold value associated with that condition:

```
[SVR:/server](def-cond-param)# threshold P1 2
```

This example will raise an alarm with a severity of P1 when the CPU goes over 2% over a period of 2 cycles.

---

The following example shows two sample alarm configurations:

```
alarm-policy default
  notify severity P1 john@cisco.com support@cisco.com
  !
   define alarm-condition CPUOverloaded
   set default-severity P2
   threshold P1 50
   threshold P2 40
   poll-cycles 2
  !
  define alarm-condition IfPacketErrors
   threshold P1 5
  !
  define alarm-condition IfAdminDown
   set default-severity P4
   disable
  !
```

# Events

All Syslog and SNMP trap events received by Cisco E-DI from the network are automatically archived in the database.

By default, the database has the capacity to store 1 million events. This limit can be increased up to 10 million events. See Configuring Event Size Restriction for more details. Events are also published by Cisco E-DI to northbound interfaces.

Cisco E-DI provides CLI commands to perform the following actions on the events:

- View all events by device or group
- Filter events based on a regular expression
- Delete events based on device or group or a time limit
- Attach a trigger to an event. The trigger action can be any Cisco E-DI command or perl script.

Cisco E-DI also listens for certain events, and performs automatic actions such as data synchronization or local status update.

To setup Cisco E-DI to listen for Syslog notifications from the NEs enter:

```
[SVR:/server} (config)# subscribe syslog
```

**Note** The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

Cisco E-DI also listens for Syslog notifications from Syslog servers on the network.

**Note** Cisco E-DI will receive and process Syslog messages corresponding to linkup and linkdown notifications. SNMP traps for linkup and linkdown are received, and archived, but not processed.

Events can be summarized, queried, and cleared based on a timestamp. Event triggers can be defined to look for a particular type of content in the events and implement any EXEC level command. Sophisticated regular expressions can be defined to filter events and take appropriate action.

# Displaying Events

Table 9-3 gives the commands that you can use to display specific event conditions.

***Table 9-4 Commands to Display Events***

| Action | Command |
|---|---|
| To show network events in network mode and server events in server mode. This is a context sensitive command. The results are formatted. | `[NET:/network]# show events` |
| To provide events in the original format as generated on the device or Cisco E-DI. | `[NET:/network]# show events raw-format` |
| To query the server for the required number of commands. | `[NET:/network]# show events last number` |
| To query the server for the events recorded in between the dates and times specified. | `[NET:/network]# show events between yyyy mm dd hh:mm:ss yyyy mm dd` |
| To specify the number of events in the original Syslog format as generated on the device or Cisco E-DI. | `[NET:/network]# show events raw-format last number` |
| To list events for a specific device | `[NET:/network]# show events device ip_address` |
| To list specified number of events for a specific device | `[NET:/network]# show events device ip_address last number` |
| To list events for a specific group | `[NET:/network]# show events group group-name` |
| To list specified number of events for a specific group | `[NET:/network]# show events group group-name last number` |
| To summarize all events for a device | `[NET:/network]# show events device ip_address summary` |
| To summarize all events for a group | `[NET:/network]# show events group group-name summary` |
| To summarize all events for a specific by the type of facility. | `[NET:/network]# show events summary` |
| To filter events by specifying a regular expression. | `[NET:/network]# show events filter regular-expression/text in event's message` |
| To filter events by specifying a regular expression. | `[NET:/network]# show events raw-format filter regular-expression/text in event's message` |
| To clear events for the current selection of devices or server. This is a context sensitive command. | `[NET:/network]# clear events` |

*Table 9-4 Commands to Display Events (continued)*

| Action | Command |
|---|---|
| To clear all events for the network or server. This is a context sensitive command. | `[NET:/network]# clear events all [network \| server]` |
| To clear events for the network or server which are older than the specified time frame. This is a context sensitive command. | `[NET:/network]# clear events older-than [days \| hours] [1-240]` |

# Configuring an Event Trigger

An event trigger can be defined to look for a particular type of content in the events. This allows you to perform an action upon detecting a specified pattern in the events received from the network or server.

Any EXEC level task can be performed as an action, including sending an e-mail or generating an alarm. Table 9-5 details the commands to configure an event trigger to perform a specified action.

*Table 9-5 Commands to Configure an Event Trigger*

| Action | Command |
|---|---|
| To define an event trigger to perform a certain action upon detecting a network condition.<br>**Note** If you choose a name which already exists for an event trigger, the existing event trigger will be overwritten by the new event-trigger. You can list event triggers and associated parameters. | `[SRV:/server](config)# event-trigger name` |
| To apply the trigger to events generated from the server or the specified device on the network. | `[SRV:/server](conf-evt-trig)# domain {network {ip_address1 ip_address2}\| server}` |
| To specify a pattern to be matched. Option to match all or any of the regular expressions specified. | `[SRV:/server](conf-evt-trig)# pattern [match-all \| match-any] regular-expression` |
| To implement the specified **exec** level commands when a successful match of the pattern occurs. | `[SRV:/server](conf-evt-trig)# execute [exec-level-command-1; exec-level-command-2…]` |
| To list all the configured event triggers and the associated parameters. | `[SRV:/server]# show server running-config module event-triggers`<br>or<br>`[SRV:/server]# show running-config` |
| To delete an event trigger. | `[SRV:/server](config)# no event-trigger name` |

The following example shows a sample event trigger:

```
event-trigger MemoryTrigger
  pattern match-all MALLOC-FAIL
  execute show alarms | email john@cisco.com
```

# Configuring Event Size Restriction

Events are stored in the Cisco E-DI database. The number of events stored can be configured. Once the number of events cross the specified size, 10% of the recent events are automatically deleted.

To configure the number of events to be stored:

**Step 1** Login to the Cisco E-DI server with administrative privileges.

**Step 2** Enter into the configure mode:

```
[SVR:/server]# config terminal
```

**Step 3** Enter the following command to define the maximum number of events to be stored:

```
[SVR:/server](config)# events server | network max-size number
```

**Step 4** Enter this command to verify that the running configuration shows the maximum number of events:

```
[SVR:/server]# show running-config | include event
```

CHAPTER 10

# Using Perl Scripts

Cisco E-DI supports Perl scripting through the CLI. This feature automates many of the server and network administration tasks.

Each invocation of a Perl script will use an additional CLI session for the duration of that script implementation.

This section includes the following information:



# Perl Script Examples

This section includes the following examples:



These examples are available under *Cisco E-DI Install Location*\Cisco-EDI\perl\perl-samples on both Windows and Linux, where, *Cisco E-DI Install Location* is the directory in which Cisco E-DI is installed.

## Verifying a Perl Script

Perl script to verify that any Perl script that is run returns correct **getresponse**, **getstatuscode** and **getstatusmessage** messages:

```
use lib '/perlapi';
use JMSPERLAPI;
$| = 1;
my $api= JMSPERLAPI->getAPI ();
$api->executeCMD ("show version");
$code=$api->getStatusCode ();
$output=$api->getResponse ();
$stMesage=$api->getStatusMessage();
print "\status Code is: $code \n";
print "\Response from JMS is: \n $output \n";
print "\n Status Message is: $stMesage \n";
$api->closeAPI ();
```

When this Perl script is run, the expected output is as follows:

```
admin@edi-test-dell_blr_19[SVR:/server]# perl /server/def.pl
status Code is: 0
Response from JMS is:
 Cisco Enhanced Device Interface Server, version 2.0
Copyright (C) 2005 Cisco Systems Inc. All rights reserved.
Compiled on 3-June-2005 by buildserver

Uptime 0 days 5:32:46, effective user admin
Server is running on system edi-test-dell_blr_19 with OS Linux (i386) 2.6.9-5.ELsmp
Number of processors detected: 1
Java runtime environment version 1.4.2_03

Status Message is: OK

!Status Code: 0
```

# Verifying the HTTP Server is Enabled on Cisco IOS Devices

This script checks whether the HTTP server is enabled on any of the Cisco IOS devices that are being managed by Cisco E-DI.

```
use lib '/perlapi';
use JMSPERLAPI;
$| = 1;
my $api= JMSPERLAPI->getAPI ();

($code, $output) = $api->executeCMD ("show devices");
if ($code != 0) {
    print "failed to retrieve device list.\n";
    exit;
}

@temp = split(/\n/,$output);  # Taking ouput into an array
foreach $line (@temp) {
    if(defined($line)){
        $line=~m/(\s+|\S\s)(\d+\.\d+\.\d+\.\d+)(.*)/;
        if($1 !~m/\*/) {
            # if it is a supported device

            if (defined($2)) {
                $device=$2;
                ($code, $cmdout) = $api->executeCMD ("network $device");
                if ($code != 0){
                    print "Could not change context to $device";
                    next;
                }

                ($code, $devOS) = $api->executeCMD ("show report software");
                $devOS =~m/(\s)(\d+\.\d+\.\d+\.\d+)(\s+)(\w+)(\s+)(\w+)(.*)/;
                $OS = "$6";
                if( $OS =~m/IOS/){
                    # If IOS, Check whether http is enabled
                    ($code, $runConfig) = $api->executeCMD ("show running-config | include
        \"ip http server\"");
                    if($runConfig =~/\s\sip\shttp\sserver/){
                        print"Http Service is enabled on the device: $device\n";
                    }
                }
            }
```

```
        }
    }
}

$api->closeAPI ();
```

# Verifying NTP Server Configuration and Enforcing the Policy

This script is used to verify bulk configuration changes to NEs with Cisco IOS Version. The script parses data from the **show devices** output and displays the supported devices including Cisco IOS and CatOS devices.

For Cisco IOS devices, it first checks if the NTP server is configured. If the NTP server is not configured, the script will configure the server with the specified IP address.

For devices where the NTP server is already configured, it checks the IP address with the specified one. If these do not match, the script will configure the server with the specified IP address.

The variables are as follows:

- @Device_info—Displays the parsed **$output** content.
- @Dev_List—Lists the Cisco E-DI supported devices including Cisco IOS and CatOS.
- @IOS_DEVICES—Lists the Cisco E-DI supported Cisco IOS Devices.
- @CatOS_DEVICES—Lists the Cisco E-DI supported CatOS Devices.

```
use lib '/perlapi';
use JMSPERLAPI;
$| = 1;

# IP Address of the NTP Server (Change the value below to required address)
$address = "1.1.1.1";

$dev = 0;
$ios = 0;
$catos = 0;

my $api= JMSPERLAPI->getAPI();
($code, $output) = $api->executeCMD("show devices ");
$output =~ s/^\s+//;

###Parsing The Output of 'show Devices'

@Device_info = split(/[\n]/, $output);

###Read Devices One by One and Extract EDI
###Supported Devices including IOS and CatOS

foreach $i (@Device_info) {
    if(defined($i)) {
        $i =~ m/(\s+|\S\s)(\d+\.\d+\.\d+\.\d+)(.*)/;
        if($1 !~m/\*/) {
            if(defined($2)) {

                @Dev_List[$dev] = "$2";
                ($code, $Ver_OS) = $api->executeCMD("show report software | include
                $Dev_List[$dev] ");

                ###Followind code Seperats the IOS and CatOS Devices
                $Ver_OS =~m/(\s)(\d+\.\d+\.\d+\.\d+)(\s+)(\w+)(\s+)(\w+)(.*)/;
```

```
        ### For IOS Devices Check the following Conditions
        ### 1.Whether NTP Server configured if so with specified IP
        ### if not Remove the existed IP and Configure with specified IP
        ### 2.If no NTP server Configured ,Configure with specified IP

        $tmp = "$6";
        if( $tmp =~m/IOS/) {
            @IOS_DEVICES[$ios++] =  "$Dev_List[$dev]";
            ($code, $cmdout) = $api->executeCMD("network $Dev_List[$dev]");
            ($code, $check_ntp) = $api->executeCMD("show running-config | include
ntp");
            if($check_ntp  =~ m/(\s+)(ntp\sserver)(.*)/)  {
                $existed_ip ="$3";
                if($3 !~ m/($address)/)  {
                    print "NTP Server Configuration changing from $3\n";
                    print "  to $address on $Dev_List[$dev], please wait ...\n\n";

                    ($code, $cmdout) = $api->executeCMD("config setup");
                    ($code, $cmdout) = $api->executeCMD("configure");
                    if ($code != 0) {
                        print "Unable to enter configure mode of $Dev_List[$dev],
skipping the device";
                        next;
                   }
                    ($code, $cmdout) = $api->executeCMD("no ntp server
$existed_ip");
                    ($code, $cmdout) = $api->executeCMD("ntp server $address");
                    ($code, $cmdout) = $api->executeCMD("exit");
                    ($code, $status) = $api->executeCMD("commit"); #  Committing
the change to the device
                    if($status =~ m/\[OK(.*)\]/) {
                        print "\n NTP Server Successfully Configured on
$Dev_List[$dev]\n\n";
                    } else {
                        print "\n No Response From  Device....$Dev_List[$dev]\n";
                    }

                    ($code, $cmdout) = $api->executeCMD("exit");
                    ($code, $cmdout) = $api->executeCMD("server");
                } else {
                    print "Specified NTP Server Configuration Already Present On
:$Dev_List[$dev]\n\n";
                    ($code, $cmdout) = $api->executeCMD("server");
                }
            } elsif ($check_ntp =~ m/(\[$Dev_List[$dev]\]\sWARNING:)(.*)/) {
                print "Device $Dev_List[$dev] offline\(Running config not
available\).....!\n\n";
                ($code, $cmdout) = $api->executeCMD("server");
            } else {
                print "Configuring NTP Server on $Dev_List[$dev]...plz Wait.! \n";
                ($code, $cmdout) = $api->executeCMD("config setup");
                ($code, $cmdout) = $api->executeCMD("configure");
                ($code, $cmdout) = $api->executeCMD("ntp server $address");
                ($code, $cmdout) = $api->executeCMD("exit");
                ($code, $status) = $api->executeCMD("commit");

                if($status =~ m/\[OK(.*)\]/) {
                    print "NTP Configured successfully....On : $Dev_List[$dev]
\n\n";
                } else {
                    print "\nfailed to configure device: $Dev_List[$dev]\n\n";
                }
                ($code, $cmdout) = $api->executeCMD("exit");
```

```
                        ($code, $cmdout) = $api->executeCMD("server");
                    }
                } else {
                @CatOS_DEVICES[$catos++] =  "$Dev_List[$dev]"; }
            }
        }
    }
    $dev++;
}


$api->closeAPI();

1;
```

# Verifying Password Encryption is Disabled on Cisco IOS Devices

This script can be used to check whether password encryption service is disabled on Cisco IOS devices that are being managed by Cisco E-DI.

```
use lib '/perlapi';
use JMSPERLAPI;
$| = 1;

my $api= JMSPERLAPI->getAPI();

($code, $output) = $api->executeCMD ("show devices");

@temp = split(/\n/,$output);
foreach $line (@temp) {
    if(defined($line)){
        $line=~/(\s)(\d+\.\d+\.\d+\.\d+)(.*)/;
        if($2 =~m/(\d+\.\d+\.\d+\.\d+)(.*)/){
            if (defined($1)) {
                $device=$1;
                print "Verifying for Device: $device....\n";
                $api->executeCMD ("network $device");
                if ($code != 0) {
                    print "Unable to change the context to device $device\n";
                    next;
                }
                $api->executeCMD ("show report software");
                $devOS = $api->getResponse();
                $devOS =~m/(\s)(\d+\.\d+\.\d+\.\d+)(\s+)(\w+)(\s+)(\w+)(.*)/;
                $OS = "$6";
                if( $OS =~m/IOS/) {
                    ($code, $output) = $api->executeCMD ("show running-config | include
        \"no service password-encryption\"");
                if($output=~/no\sservice\spassword-encryption/) {
                   print"Password Encryption is Disabled on the device: $device\n";
                }
                }
            }
        }
    }
}

$api->closeAPI();
```

CHAPTER 11

# Creating and Using Macro Commands

The Macro command feature of E-DI helps you to define device and OS-independent commands.

A Macro command provides an abstraction for command sets and/or command variations. In a single operation, you can download commands to various types of platforms that have variation in CLI commands. In this way, Macro commands make it easier for you to deal with variations across OS versions and platforms for configuration changes.

This feature is available for IOS, Cat OS and PIX platforms.

E-DI contains simple macros for a set of commands that have different variations on different platforms. These Macro commands are packaged along with E-DI. You an also create your own macros.

The macros contain simple keywords and command parameters similar to template variables. If you enter these keywords and parameters, the internal syntactical and semantic differences among various devices, OS types, and versions are handled internally by E-DI.

Each Macro command that is defined can be translated to commands on all available device families and OS types. They can also be translated to a particular device family and OS type.

When a corresponding configlet for a particular device family is defined, E-DI verifies and translates this. If there are errors during translation, the particular macro support for that device family will not be available.

E-DI compiles the macro into macro XML files, based on the device family. E-DI then converts the macro XML files to CLI. This translation makes the command variations transparent to you.

You can create and use macros:

- Through CLI (see Creating and Using Macros Through CLI
- Through GUI (see Creating and Using Macros Through UI)

# Creating and Using Macros Through UI

Macro Command Manager is an Eclipse- based, standalone UI tool of E-DI. It allows you to create, edit, delete, and deploy macros to devices.

To launch macro Command Manager, see Launching Macro Command Manager

# Launching Macro Command Manager

Macro Command Manager is packaged with Cisco E-DI, and will be available after you have installed Cisco E-DI. To install Cisco E-DI, see:

- *Installation Guide and Setup Guide for Enhanced Device Interface, 2.2 on Windows*
- *Installation Guide and Setup Guide for Enhanced Device Interface, 2.2 on Linux*

**Note** Before you start Macro Command Manager, ensure that the EDI Service is running.
To start this service, On Windows, go to **Start > Programs > Cisco E-DI > E-DI Service > Start**.
On Linux, navigate to *E-DI Install Location* /Cisco-EDI/bin and enter `./start` at the command prompt.

Before you launch Macro Command Manager: (These steps are optional.)

**Step 1** Go to the command prompt and navigate to your Eclipse folder (where `eclipse.exe` resides).

**Step 2** Run the command `eclipse -clean`

This ensures that the cache is cleaned.

Follow these steps to launch Macro Command Manager:

**Step 1** On Windows:

- Choose **Start > Programs > Cisco E-DI > E-DI Service > Device Configuration Manager**.
- or
- Navigate to the directory *E-DI Install Location*\Cisco EDI\edi\dist\ui_products\configmanager and double-click on launcher .exe.

On Linux:

- Navigate to *E-DI Install Location*/Cisco EDI/edi/dist/ui_products/configmanager and enter `./launcher`

E-DI prompts you to log in to the E-DI server.

**Step 2** Log in using the admin credentials.

Select the SSH check box if you want to run DCM in SSH mode.

By default, DCM connects to the port 2323 on the server.

If the server Telnet port is not 2323, you should change this value in the **eclipse.ini file**. This file is located in the following location:

On Windows:

*E-DI Install Location*\edi\dist\ui_products\configmanager.

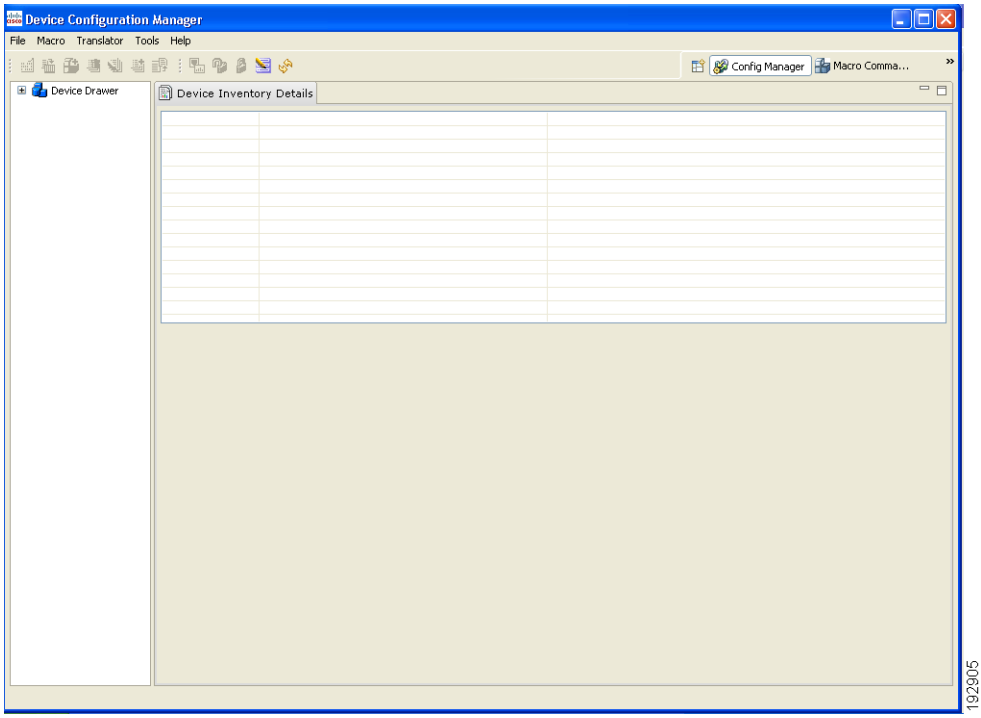
On Linux:

*E-DI Install Location*/edi/dist/ui_products/configmanager

After you log in, Device Configuration Manager opens. This has three perspectives (which appear as buttons):

- Config Manager—This is the default perspective, and this button is highlighted. See Figure 11-1
- Macro Command Manager—Opens the Macro Command Manager perspective. See Figure 11-1
- Command Translator—Opens the Command Translator perspective. To display the Command Translator button, click on the >> symbol that appears after the Macro Command Manager Button. See Figure 11-1.

***Figure 11-1 Device Configuration Manager default perspectives and the >> symbol***




**Step 3** Click **Macro Command Manager.**

The Macro Command Manager perspective opens and you see the Device Drawer in the left pane.

Alternatively, to launch Macro Command Manager from the Config Manager perspective, you can click the Other icon and select Other.

The Open Perspective dialog box appears.

Select Macro Command Manager and click **OK**.

The Macro Command Manager perspective opens.

# Understanding the High-level Workflow of Macro Command Manager

This is the high-level workflow of the Macro Command Manager:

**Step 1** Create a Macro Package.

A Macro Package is a container for a set of macros. It allows you to easily organize your Macros. See Creating a Macro Command.

**Step 2** Create a Macro.

A macro contains configlets, parameters and their descriptions. Creating a Macro Command.

**Step 3** Create Configlets.

A Configlet is a command holder for device variation. It is a set of related commands meant to do a specific job on devices. Creating a Macro Command.

**Step 4** Deploy the macro.

See Deploying a Macro Command to a Device.

## Understanding the Macro Command Manager UI

To launch Macro Command Manager, see Launching Macro Command Manager.

Macro Command Manager has the following views:

- Macro Command Tree View

  Displays the Macro packages, macros and configlets in a hierchical view. A default Macro package, Root, always exists. If you right-click in the tree view, a context menu appears with these options:

  - Deploy Macro
  - Add Macro Package
  - Delete Macro Package
  - Add Macro
  - Delete Macro
  - Add Configlet
  - Delete Configlet

- Macro View

  Displays the Macro details such as the Package to which it belongs, the Macro name, the parameters and their description.

- Macro Command Editor and Config Editor View

  These views appear only when you select a Macro from the Tree view, right-click on it and then select Add Configlet.

  You can enter the details of a configlet here. The Config Editor allows you to enter commands. You can also select commands using the Config Editor.

# Creating a Macro Command

To create a Macro Command you must:

1. Create a Macro Package—see Creating a Macro Package.
2. Create a Macro—see Creating a Macro.
3. Create a Configlet—see Creating a Configlet.

## Creating a Macro Package

A default Macro Package, Root, exists in the Macro Command Tree View. You can add macros to this or create a new package.

To create a new Macro Package:

**Step 1** Go to the Macro Command Tree View, right-click and select **Add Macro Package** from the context-menu that appears.

**Step 2** Enter the package name.

**Step 3** Enter a short description for the package.

**Step 4** Click **OK**.

**Step 5** The new Macro Package appears in the Macro Command Tree View.

To delete a Macro Package, select the package, right-click on it and select **Delete Macro Package** from the context menu that appears.

## Creating a Macro

To add a Macro:

**Step 1** Go to the Macro Command Tree View, select a macro package, right-click and select **Add Macro** from the context-menu that appears.

The Macro Addition Wizard appears.

**Step 2** Expand Macro Basic Parameters.

The Package Name field is populated by default, with the selected parent package name.

The Root Package is represented by a forward slash (\). All other user created Macro Packages appear with this format: *Package_name.*

**Step 3** Enter the Macro name.

**Step 4** Expand Parameters List.

**Step 5** Enter a name for the Parameter, and add a description in the Description field.

**Step 6** Click **Add**.

The Parameter appears as a variable in the table below. The name and description details are displayed. Use the Add/Remove buttons to add another property or remove existing ones.

Click **Finish**.

---

To delete a Macro, select the macro, right-click on it and select **Delete Macro** from the context menu that appears.

## Creating a Configlet

To create a Configlet:

---

**Step 1** Go to the Macro Command Tree View, select a macro, right-click, and select **Add Configlet**.

The Macro Config Editor and Command Editor views appear.

The Macro Configlet Index is automatically populated. This cannot be changed.

**Step 2** Select the Device Family from the drop-down list.

**Step 3** Select the IOS image version from the Version drop-down list.

**Step 4** Go to the Config Editor and enter the parameterized CLI commands that you want to include in the configlet.

When you enter the parameters, specify the type of the parameter by appending `:` and the hint after parameter name. This will be automatically done if you put a colon and enter Ctrl+Space.

For example, if you have defined `$p1` as a parameter in the macro, you can use this parameter in the configlet as below:

`logging $p1:`*A.B.C.D*

**Step 5** Save the configlet by selecting it and then selecting **Configlet > Save Configlet** from the Main Menu.

The configlet appears in the Macro Command Tree View.

---

To edit an existing configlet, select it from the Tree View. The configlet details appear in the MacroCommand.Editor and Command Editor views. Change the details and save the configlet.

To delete a configlet, select it from the Tree View, right-click on it and select **Delete Configlet** from the context menu that appears.

# Deploying a Macro Command to a Device

To deploy a Macro Command to a device:

---

**Step 1** Select a Macro Package, right-click on it and select **Deploy Macros f**rom the context-menu that appears

The Deploy Macros wizard appears.

**Step 2** Enter the values for the parameters in the Configlet.

**Step 3** Click **Associate Device** to associate devices to which the macros should be deployed.

A pop-up appears.

**Step 4** Enter the Device IP and click **Go.**

Or

Select the devices from the Device Drawer.

**Step 5** Click **OK**.

**Step 6** Click **Next** in the Deploy Macros dialog box.

The Job Scheduler dialog box appears.

You can:

- Schedule a job to deploy the macros.

  Enter a name for the job, select a date using the calendar icon, and select the time from the drop-down list box. The job will run and deploy the macros as scheduled.

  or

- Deploy the macros to the selected devices immediately. The macros will be deployed immediately.

**Step 7** Click **Finish**.

# Creating and Using Macros Through CLI

Using NetCLI when you specify a macro, use this convention:

*/packagename.macroname*

where *packagename* is the name of the macro package and *macroname* is the name of the macro.

***Table 11-1 Commands to Create Macros***

| Action | Command |
|---|---|
| To enter macro configuration mode.<br>Displays a message:<br>`Entering Macro Configuration mode.`<br>In the macro configuration mode you have the following options:<br>• `compile–`<br>• `delete`<br>• `end`<br>• `exit`<br>• `export`<br>• `import`<br>• `macro`<br>• `new`<br>• `show` | *user*`@`*server*`[SVR:/]#` **`configure macro`**<br>Displays a message:<br>`Entering Macro Configuration mode.`<br>The prompt changes to *user*`@`*server*`[SVR:/]<macro># ?`<br>`[compile \| delete \| end \| exit \| export \| import \| macro \| new \| show ]` |
| To create a macro package or a macro. | *user*`@`*server*`[SVR:/<macro>]#` **`new`** `[ macro \| package ]` |

*Table 11-1 Commands to Create Macros (continued)*

| Action | Command |
|---|---|
| To create a new package. | *user*@*server*`[SVR:/<macro>]#` **`new package`** *packagename*<br>where *packagename* is a name of your new macro package<br>This message appears:<br>`You are creating a new package. Entering Macro Configuration mode.` |
| To create a new macro. | *user*@*server*`[SVR:/<macro>]#` **`new macro`** *macroname*<br>where *macroname* is a name of your new macro.<br>You are creating a new macro. Entering Macro Configuration mode.<br>The prompt changes to:<br>*user*@*server*`[SVR:/](macro-edit)#[ configlet \| end \| exit \| keyword \| param \| show]` |
| To create a new configlet. | *user*@*server*`[SVR:/](macro-edit)#`**`configlet`** *ConfigletIndex* **`scope`** *DeviceFamily ImageVersion*<br>*Configlet Index* is the index of the configlet that you are creating. Select from 1 to 99.<br>**`scope`** is the scope of the configlet with regard to the device family and OS version.<br>*DeviceFamily* is the device family.<br>*ImageVersion* is the image version for that device family.<br>This message appears:<br>`You are creating a new configlet. Entering Configlet Configuration mode.`<br>Now specify the commands for the configlet. Use ? to view and select commands. After you are done press Enter.<br>The prompt changes to include the device family-OS version pair that you selected. For example, *user*@*server*`[SVR:/](Cisco7600-12.2(18)SXD4-configlet)`<br>Now specify the parameters, for example $parameter 1, $parameter 2, etc., and press Enter.<br>EDI matches your configlet with the device packages. If successfully matched, you will see the result as *MATCHED* |

*Table 11-1 Commands to Create Macros (continued)*

| Action | Command |
|---|---|
| To edit a macro. | *user@server*`[SVR:/<macro>]#` **`macro`** *macroID*<br>where *macroID* is the name/ID of the Macro that you want to edit.<br>These details of the Macro appear:<br>• Keyword and description.<br>• Parameters, and their description.<br>Then the following message appears:<br>`Entering Macro` *macroID*<br>where *macroID* is the name/ID of the Macro that you want to edit<br>The prompt changes to *user@server*`[SVR:/<macro-edit>]# [ configlet \| end \| exit \| keyword \| param \| show ]`<br>To edit, follow the same processes used while creating a macro. |
| To convert the macro into the ED-I CLI XML models.<br>After compilation, your XML file appears in this location:<br>*CiscoEDI Install Location*/Cisco E-DI/edi/resources/server/macro<br>where *CiscoEDI Install Location* is the location where E-DI is installed.<br>This feature is not supported through GUI. | *user@server*`[SVR:/<macro>]#` **`compile`** *packagename*<br>where *packagename* is a macro package.<br>Upon successful compilation, the following message appears:<br>`Package Compiled into` *CiscoEDI Install Location*`/Cisco E-DI/edi/resources/server/macro` |
| To export a macro to an XML file.<br>This feature is not supported through GUI. | *user@server*`[SVR:/<macro>]#` **`export`** *macro_package_name XMLfilename*<br>where *macro_package_name is the name of the macro package to be exported*<br>and *XMLfilename* is the name of the XML file to which the macro package needs to be exported.<br>For example, if you enter:<br>*user@server*`[SVR:/<macro>]#` **`export`** *logging logging.xml*<br>the Macro package named *logging* is exported to the file *logging.xml* |
| To import a macro from an XML file.<br>This feature is not supported through GUI. | *user@server*`[SVR:/<macro>]#` **`import`** *filename*<br>where *filename* is the name of the XML file from which the macro needs to be imported. |
| To delete a package or a macro. | *user@server*`[SVR:/<macro>]#` **`delete macro`** *packagename*<br>where *packagename* is the name of the package.<br>or<br>*user@server*`[SVR:/<macro>]#` **`delete macro`** *macroname*<br>where *macroname* is the name of the macro. |

*Table 11-1 Commands to Create Macros (continued)*

| Action | Command |
|---|---|
| To view macro packages, macro lists, or macro details. | *user*@*server*[SVR:/<macro>]# **show** [details \| list \| packages] |
| To view details of macro.<br>For a given macro, these details are displayed:<br>• Keyword and description.<br>• Parameters, and their description. | *user*@*server*[SVR:/<macro>]# **show details** *Macro ID*<br>where Macro ID is the name of the Macro.<br>For example:<br>*user*@*server*[SVR:/<macro>]# **show details** *log*<br>shows you the details about the macro with name/ID as *log*. |
| To view the list of Macros.<br>These details appear in a tabular format:<br>• Packages<br>• The associated Macro IDs (names of macro)<br>• Parameters associated with each Macro ID. | *user*@*server*[SVR:/<macro>]# **show list** |
| To view the list of macro packages.<br>These details are displayed:<br>• The list of macro packages<br>• The number of macros associated with each package.<br>The root package (default) is represented by / | *user*@*server*[SVR:/<macro>]# **show packages** |

CHAPTER 12

# Translating Commands Using Command Translator

Cisco EDI Command Translator enables you to translate Cisco Catalyst Operating System (CatOS) configurations to equivalent supported Cisco IOS® configurations.

This is because configuration management and network migration systems, need differentiated configuration applications to handle complex network transitions.

The Command Translator provides targeted Cisco IOS configuration for a given CatOS configuration file. This application enables network administrators who have expertise in CatOS configuration commands to learn Cisco IOS configuration commands.

The Command Translator increases productivity, even if you are not familiar with the Cisco IOS configuration commands.

| Feature | Benefit |
|---|---|
| QoS command output based on module presence on the device. | Helps to learn QoS configuration commands based upon various module QoS configurations. |
| Edit CatOS configurations | Allows you to simultaneously edit changes to CatOS configuration files in order to compare Cisco IOS. |

This section has the following topics:

# Components Used

The information in this document is based on these software and hardware versions:

- CatOS version 8.5.1 and earlier
- Cisco IOS Software Release 12.2.18SXF3
- Cisco IOS Software Release 12.2.18.SXF5

**Note** If your network is live, make sure that you understand the potential impact of any command.

# Prerequisites

Complete these key steps in order to plan a migration from CatOS to Cisco IOS:

- Verify the hardware and software support for the new system:
  - Cisco IOS images typically require larger amounts of flash memory.
  - Use the release notes in order to verify the line card and feature set support in the target image.
- Understand these operational differences:
  - System image name conventions and boot file locations
  - Management network interfaces
  - QoS behavior
  - VLAN Trunking Protocol

# Launching Command Translator

Command Translator is packaged with Cisco E-DI, and will be available after you have installed Cisco E-DI. To install Cisco E-DI, see:

- *Installation Guide and Setup Guide for Enhanced Device Interface, 2.2 on Windows*
- *Installation Guide and Setup Guide for Enhanced Device Interface, 2.2 on Linux*

**Note** Before you start Command Translator, ensure that the EDI Service is running.
To start this service:
On Windows, go to **Start > Programs > Cisco E-DI > E-DI Service > Start**.
On Linux, navigate to *E-DI Install Location* /Cisco-EDI/bin and enter **`./start`** at the command prompt.

Before you launch Command Translator: These steps are optional.

**Step 1** Go to the command prompt and navigate to your Eclipse folder (where **`eclipse.exe`** resides).

**Step 2** Run the command **`eclipse -clean`**

This ensures that the cache is cleaned.

Follow these steps to launch Command Translator:

**Step 1** On Windows:

- Choose **Start > Programs > Cisco E-DI > E-DI Service > Device Configuration Manager**.

Or

- Navigate to the directory *E-DI Install Location*\Cisco EDI\edi\dist\ui_products\configmanager and double-click on **`launcher .exe`**.

On Linux:

- Navigate to *E-DI Install Location*/Cisco EDI/edi/dist/ui_products/configmanager and enter **`./launcher`**

E-DI prompts you to log in to the E-DI server.

**Step 2** Log in using the admin credentials.

Select the SSH check box if you want to run DCM in SSH mode.

By default, DCM connects to the port 2323 on the server.

If the server Telnet port is not 2323, you should change this value in the **eclipse.ini** file. This file is located in the following location:

- On Windows: *E-DI Install Location*\edi\dist\ui_products\configmanager.
- On Linux: *E-DI Install Location*/edi/dist/ui_products/configmanager

After you log in, Device Configuration Manager opens. This has three perspectives (which appear as buttons):

- Config Manager—This is the default perspective, and this button is highlighted. See Figure 12-1.
- Macro Command Manager—Opens the Macro Command Manager perspective.
- Command Translator—Opens the Command Translator perspective. To display the Command Translator button, click on the **>>** symbol that appears after the Macro Command Manager Button. See Figure 12-1. After you click on **>>**, the Command Translator button appears. See Figure 12-2

*Figure 12-1 Device Configuration Manager default perspectives and the >> symbol*

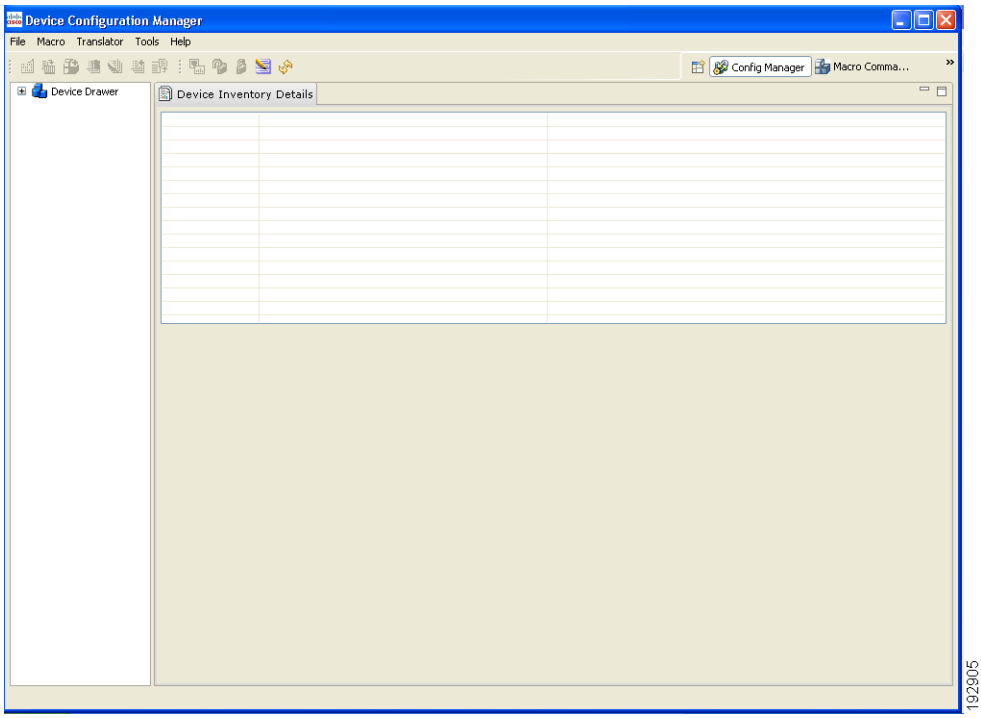
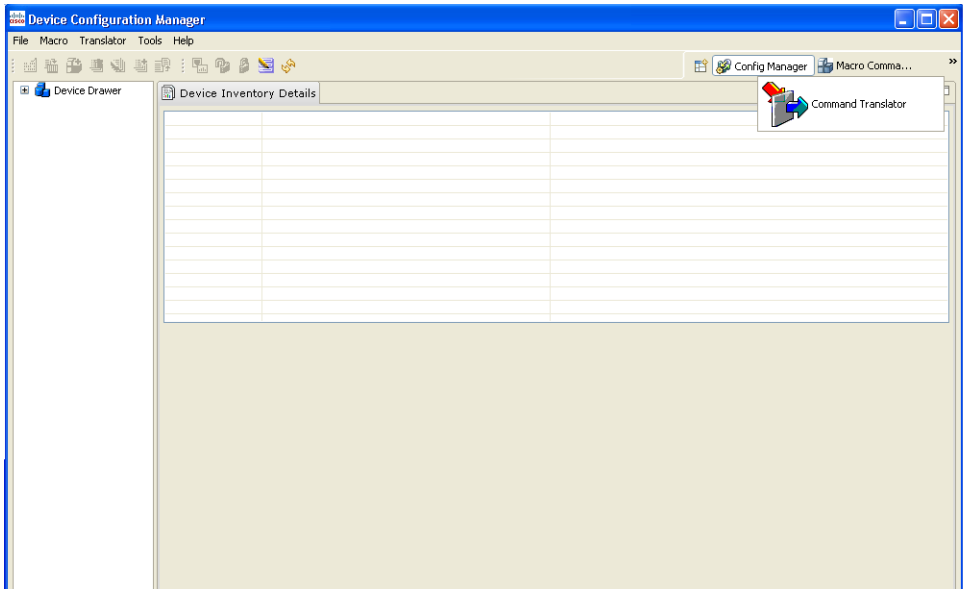



*Figure 12-2 The Command Translator button appears*




**Step 3** Click **Command Translator.**

The Command Translator perspective opens.

# Using the Command Translator

You can load the configuration file into Command Translator translate a CatOS configuration into a Cisco IOS configuration.

To do this:

**Step 1** Launch Command Translator. See Launching Command Translator.

**Step 2** From the Main Menu, select **Translator > Open File** to open the configuration file that you want to translate.

The file appears in the left pane.

**Step 3** Select the source OS version from the Source OS drop-down box.

**Step 4** Select the target OS from the Target OS drop-down box.

If you need to add hardware related information that is required for the translation, click on Include Show Module Output. A text box appears and you can paste or enter your hardware related information into this box.

**Step 5** Select and output format that is displayed as ordered or line by line. Even after the translation is complete, you can toggle between the line by line format and the ordered format.

**Step 6** Click the **Translate** button.

**Step 7** The translated configuration appears in the right pane.

Green color indicates commands that are properly translated.

Red color indicates the commands that are not properly translated.

# Untranslated CatOS Commands

This section contains a list of the CatOS commands which are not translated by the Command Translator.

```
set authorization <enable |commands |exec> disable [<both |console |telnet>]
set authorization <enable |commands |exec> <enable|config|all>
<if-authenticated|none|tacacs+>
-------------------------------------------------------------------------------
set boot auto-config <device:file_name> [<mod>]
-------------------------------------------------------------------------------
set boot device <bootdevice[:bootdevice-qualifier]>[,bootdevice[:bootdevice-qualifier]] [
-------------------------------------------------------------------------------
set boot config-register auto-config sync <enable|disable>
set boot config-register auto-config <recurring|non-recurring> [<mod>]
set boot config-register auto-config <append|overwrite>
set boot config-register baud <9600|4800|38400|19200> [<mod>]
set boot config-register boot <bootflash|rommon|system> [<mod>]
set boot config-register ignore-config <enable|disable> [<mod>]
set boot config-register <value> <mod>
-------------------------------------------------------------------------------
set boot sync now
set boot sync timer <time>
-------------------------------------------------------------------------------
set boot system flash <device:file_name> prepend [<mod>]
-------------------------------------------------------------------------------
set cam <dynamic> <mac_address> <port-list> [<vlan>]
```

```
--------------------------------------------------------------------------------
set cam dynamic filter <mac_address> <vlan> @vasu
--------------------------------------------------------------------------------
set cam notification added <enable|disable> <port-list>
set cam notification removed <enable|disable> <port-list>
set cam notification threshold <enable|disable>
set cam notification threshold interval <120..4294967295>
set cam notification threshold limit <0..100>
set cam notification historysize <0..500>
set cam notification interval <time>
--------------------------------------------------------------------------------
set cdp version v1
set cdp format device-id <mac-address|other>
--------------------------------------------------------------------------------
set config acl nvram
--------------------------------------------------------------------------------
set config checkpoint device <device>
set config checkpoint name <name> device <device>
set config checkpoint
--------------------------------------------------------------------------------
set config rollback <name>
--------------------------------------------------------------------------------
set config mode binary
set config mode text nvram
set config mode text <device:file-id>
set config mode text auto-save <enable|disable>
set config mode text auto-save interval <time-min>
--------------------------------------------------------------------------------
set errdisable-timeout <enable|disable>
[ bcast-suppression |
cam-monitor |
crossbar-fallback |
duplex-mismatch |
gl2pt-ingress-loop |
gl2pt-threshold-exceed |
gl2pt-cdp-threshold-exceed|
gl2pt-stp-threshold-exceed|
gl2pt-vtp-threshold-exceed|
link-inerrors |
link-rxcrc |
link-txcrc |
packet-buffer-error |
other |
all ]
--------------------------------------------------------------------------------
set errordetection inband <enable|disable>
--------------------------------------------------------------------------------
set errordetection link-errors <enable|disable>
set errordetection link-errors action <errordisable|port-failover>
set errordetection link-errors interval <time>
--------------------------------------------------------------------------------
set errordetection link-errors threshold <inerrors|rxcrc|txcrc> [[high <value>] low
<value>]
set errordetection link-errors threshold <inerrors|rxcrc|txcrc> [[low <value>] high
<value>]
--------------------------------------------------------------------------------
set errordetection link-errors sampling <count>
--------------------------------------------------------------------------------
set errordetection memory <enable|disable>
--------------------------------------------------------------------------------
set errordetection portcounters <enable|disable>
--------------------------------------------------------------------------------
set interface sc0 dhcp <release|renew>
set interface <sc1|sl0> <up|down>
```

```
set interface <sc1> [<vlan>] <<<ip_addr> [<ip_mask>]> | <<ip_addr/ip_mask>
[<bcast_addr>]>>
set interface trap <sc1|sl0> <enable|disable>
set interface sl0 <slip_addr> <ip_addr>
--------------------------------------------------------------------------------
set ip fragmentation <enable|disable>
set ip permit redirect <enable|disable>
set ip unreachable <enable|disable>
--------------------------------------------------------------------------------
set lcperroraction <ignore|operator|system>
--------------------------------------------------------------------------------
set localuser authentication <disable|enable>
--------------------------------------------------------------------------------
set logging callhome <enable|disable>
set logging callhome severity <0..7>
set logging level <all | acl | callhome | cdp | cops | dhcp-snooping |
diag | dtp | dvlan | earl | ethc | filesys | gl2pt |
gvrp | ip | kernel | ld | mcast | mgmt | mls | protfilt |
pruning | privatevlan | qos | radius | rsvp | security |
snmp | spantree | sys | tac | tcp | telnet | tftp |
trace | udld | vmps | vtp> <1..7> [default]
set logging <session |telnet> <enable|disable>
--------------------------------------------------------------------------------
set module autoshut <enable |disable> <mod>
set module name <mod> [ <name> ]
set module shutdown <all |<mod>>
--------------------------------------------------------------------------------
set protocolfilter <enable|disable>
--------------------------------------------------------------------------------
set pvlan <primary_vlan> <secondary_vlan> sc0
--------------------------------------------------------------------------------
set qos acl default-action trust-override <enable |disable>
set qos acl default-action ip <trust-cos |trust-dscp |trust-ipprec | <dscp <0..63>>>
[[microflow <micro_policer_name>] aggregate <agg_policer_name>] [input |output]
set qos acl default-action mac <<dscp <dscp>> | trust-cos>
[aggregate <agg_policer_name>] [input |output]
set qos acl mac <acl-name> <<dscp <dscp>> |trust-cos>
[aggregate <agg_policer_name>]
< any | <mac_address> | host <mac_address> >
< any | <mac_address> | host <mac_address> >
[ <0x0, 0x05ff - 0xffff> |
aarp | banyan-vines-echo | dec-mop-dump | dec-mop-remote-console |
dec-phase-iv | dec-lat | dec-diagnostic-protocol | dec-lavc-sca |
dec-amber | dec-mumps | dec-lanbridge | dec-dsm | dec-netbios |
dec-msdos | ethertalk | ipv4 | ipx-arpa | xerox-ns-idp ]
[vlan <vlan>] [cos <cos>] [capture] [before | modifiy <position>]
--------------------------------------------------------------------------------
set qos autoqos
set qos cos-cos-map <cos1> <cos2> <cos3> <cos4> <cos5> <cos6> <cos7> <cos8>
set qos mac-cos <mac_addr> <vlan_list> <cos>
set qos policy-source <cops|local>
set qos rsvp <disable|enable>
set qos rsvp local-policy <forward|reject>
set qos rsvp policy-timeout <1-65535>
--------------------------------------------------------------------------------
set port qos <port-list> autoqos trust <cos|dscp>
set port qos <port-list> autoqos voip <ciscoipphone|ciscosoftphone>
set port qos <port-list> policy-source <cops|local>
set port qos <port-list> trust-device <ciscoipphone|none>
--------------------------------------------------------------------------------
set rspan disable <source|destination> session <session-num>
--------------------------------------------------------------------------------
set security acl adjacency <name> <vlan> <dest_mac_address>
[[<src_mac_address>] mtu <size>]
```

```
--------------------------------------------------------------------------------
set security acl cram auto [<sec>]
set security acl cram <run|testrun>
--------------------------------------------------------------------------------
set security acl statistics < all | <acl-name> >
set security acl feature ratelimit <rate>
set security acl log maxflow <flows>
--------------------------------------------------------------------------------
set security acl arp-inspection address-validation enable [drop [log]]
set security acl arp-inspection address-validation disable
--------------------------------------------------------------------------------
set security acl ip <acl-name> <eapoudp |url-redirect> [<before |modify> <position>]
set security acl ip <acl-name> <permit |deny> arp-inspection [log] [<before|modify>
<position>]
set security acl ip <acl-name> <permit |deny> auto-fragment
--------------------------------------------------------------------------------
set security acl map <acl_name> <port-list> [ statistics <enable |disable> ]
--------------------------------------------------------------------------------
set snmp community-ext <community_string> <read-only|read-write|read-write-all>
[view <name>] [ access <number> ]
set snmp inform <<hostname> | <ip-address> > <recvr-comm-string>
[port <port>] index <index>
set snmp rmon <enable|disable>
set snmp trap <enable |disable>
[<$trap = autoshutdown |callhomestp |entityfru |inlinepower |ippermit
|l2tunnel |linkerrhigh |linkerrlow | |noauthfailvlan
|noguestvlan |redundancy |system |sysinfolog |vmps>]
set snmp community <read-only|read-write|read-write-all>
set snmp community read-write-all <string>
set snmp community index < <indexname> | "-hex <hexformat>" >
name < <comm-string> | "-hex <hexformat>" >
security < <sec-string> | "-hex <hexformat>" >
[context < <context-string> | "-hex <hexformat>" > ]
[volatile|nonvolatile]
[transporttag < [<tag-value>]+ | "-hex [<hexformat>"]+ >]
set snmp targetaddr < <addrname> | "-hex <hexformat>" >
param < <paramname> | "-hex <hexformat>" > <ip_addr>
[ ipmask < <value> | "-hex <hexformat>" > ]
[ maxmsgsize <value> ] [ retries <value> ] [ timeout <value> ]
[ volatile|novolatile] [taglist [<tag> | "-hex <hexvalue>"]+ ]
notes: need "show snmp targetaddr" output
set snmp access < <groupname> | "-hex <hexformat>" > security-model
v3 <authentication|noauthentication|privacy>
context < <groupname> | "-hex <hexformat>" > prefix
[notify < <groupname> | "-hex <hexformat>" >]
[read < <groupname> | "-hex <hexformat>" >]
[write < <groupname> | "-hex <hexformat>" >]
[volatile|nonvalatile]
set snmp notify < <notifyname> | "-hex <hexformat>" >
tag < <notifytag> | "-hex <hexformat>" >
[<inform|trap> <volatile|novolatile>]
notes: need "show snmp notify" output
set snmp extendedrmon netflow <enable|disable> <mod>
set snmp alias <ifIndex> <ifAlias>
set snmp rmonmemory <0..100>
--------------------------------------------------------------------------------
set span permit-list <enable|disable>
set span permit-list <port-list> <include|exclude>
--------------------------------------------------------------------------------
set spantree bpdu-filter <port_list> default
set spantree bpdu-guard <port_list> default
set spantree bpdu-skewing <port_list> <enable|disable>
set spantree channelvlancost <channel_id> <cost>
set spantree defaultcostmode <short|long>
```

```
set spantree enable mistp-instance all
set spantree enable mistp-instance <mistp_instance_list>
set spantree fwddelay <fwd_delay 4..30> mistp-instance <mistp_instance_list>
set spantree hello <hello 1..10> mistp-instance <mistp_instance_list>
set spantree link-type <port_list> auto
set spantree maxage <maxage 6..40> mistp-instance <mistp_instance_list>
set spantree mode <mistp|mistp-pvst+>
set spantree mst link-type <port_list> auto
set spantree portinstancecost <port_list> cost <cost> <mistp_instance_list>
set spantree portinstancecost <port_list> <mistp_instance_list>
set spantree portinstancecost <port_list> cost <cost>
set spantree portinstancepri <port_list> <priority> <mistp_instance_list>
set spantree portinstancepri <port_list> <priority>
set spantree priority <priority> mistp <instance_list mistp>
set spantree priority <priority>
set spantree root mistp-instance <mistp_instance> [dia <diameter>] [hello <hello_time
1..10>]
-------------------------------------------------------------------------------
set system syslog-dump <enable|disable>
set system syslog-file <device:file_name>
set system countrycode [ <code> ]
set system crossbar-fallback <bus-mode|none>
set system highavailability versioning <enable|disable>
set system info-log command <command> [ <position> ]
set system info-log <disable|enable>
set system info-log interval <interval>
set system info-log <ftp|tftp> < <ip_addr> | <name> > <file>
set system info-log rcp <username> < <ip_addr> | <name> > <file>
set system modem <enable|disable>
set system profile <enable|disable> <mod>
set system profile <device:file_name>
set system redundancy-history <size>
set system supervisor-update [automatic|disable|force]
set system highavailability disable
-------------------------------------------------------------------------------
set time <day_of_week>
set time <hh:mm:ss>
set time <mm/dd/yy>
-------------------------------------------------------------------------------
set trunk <port-list> [<none | <vlan>] [<on|off|desirable|auto|nonegotiate>]
[<dot10|lane>]
-------------------------------------------------------------------------------
set vlan <vlan_list> [pvlan-type none] [ring <0x3EE .. 0xFFF>] [mistp-instance <<instance
1..set vlan <vlan-list> firewall-vlan <mod 1..9,15..16> msfc-fwsm-interface
set vlan verify-port-provisioning <enable|disable>
-------------------------------------------------------------------------------
set vtp primary [vlan|mst] [force]
set vtp pruneeligible <vlan>
set vtp version 3
set vtp mode <client|off|server|transparent> <vlan|mst|unknown>
set vtp passwd <passwd> <hidden|secret>
-------------------------------------------------------------------------------
set cops domain-name <domain-name>
set cops reconnect [diff-serv |rsvp]
set spantree enable mistp-instance <mistp_instance_list>
set spantree fwddelay <fwd_delay 4..30> mistp-instance <mistp_instance_list>
set spantree hello <hello 1..10> mistp-instance <mistp_instance_list>
set spantree link-type <port_list> auto
set spantree maxage <maxage 6..40> mistp-instance <mistp_instance_list>
set spantree mode <mistp|mistp-pvst+>
set spantree mst link-type <port_list> auto
set spantree portinstancecost <port_list> cost <cost> <mistp_instance_list>
set spantree portinstancecost <port_list> <mistp_instance_list>
set spantree portinstancecost <port_list> cost <cost>
```

```
set spantree portinstancepri <port_list> <priority> <mistp_instance_list>
set spantree portinstancepri <port_list> <priority>
set spantree priority <priority> mistp <instance_list mistp>
set spantree priority <priority>
set spantree root mistp-instance <mistp_instance> [dia <diameter>] [hello <hello_time
1..10>]
--------------------------------------------------------------------------------
set system syslog-dump <enable|disable>
set system syslog-file <device:file_name>
set system countrycode [ <code> ]
set system crossbar-fallback <bus-mode|none>
set system highavailability versioning <enable|disable>
set system info-log command <command> [ <position> ]
set system info-log <disable|enable>
set system info-log interval <interval>
set system info-log <ftp|tftp> < <ip_addr> | <name> > <file>
set system info-log rcp <username> < <ip_addr> | <name> > <file>
set system modem <enable|disable>
set system profile <enable|disable> <mod>
set system profile <device:file_name>
set system redundancy-history <size>
set system supervisor-update [automatic|disable|force]
set system highavailability disable
--------------------------------------------------------------------------------
set time <day_of_week>
set time <hh:mm:ss>
set time <mm/dd/yy>
--------------------------------------------------------------------------------
set trunk <port-list> [<none | <vlan>] [<on|off|desirable|auto|nonegotiate>]
[<dot10|lane>]
--------------------------------------------------------------------------------
set vlan <vlan_list> [pvlan-type none] [ring <0x3EE .. 0xFFF>] [mistp-instance <<instance
1..set vlan <vlan-list> firewall-vlan <mod 1..9,15..16> msfc-fwsm-interface
set vlan verify-port-provisioning <enable|disable>
--------------------------------------------------------------------------------
set vtp primary [vlan|mst] [force]
set vtp pruneeligible <vlan>
set vtp version 3
set vtp mode <client|off|server|transparent> <vlan|mst|unknown>
set vtp passwd <passwd> <hidden|secret>
--------------------------------------------------------------------------------
set cops domain-name <domain-name>
set cops reconnect [diff-serv |rsvp]
set cops retry-interval <initial> <increment> <maximum>
set cops server <ip_address> [<1-65535>] [rsva] [primary] [diff-serv]
--------------------------------------------------------------------------------
set dot1x radius-accounting <enable|disable>
set dot1x radius-keepalive <enable|disable>
set dot1x radius-vlan-assignment <enable|disable>
set dot1x shutdown-timeout <0..65535>
set dot1x vlan-group <group-name> <vlan-list>
--------------------------------------------------------------------------------
set feature <agg-link-partner|mdg> <disable|enable>
--------------------------------------------------------------------------------
set gmrp [fwdall] <enable|disable> [<port-list>]
set gmrp registration <fixec|forbidden|normal> <port-list>
set gmrp timer all <join-value> <leave-value> <leaveall-value>
set gmrp timer join <time>
set gmrp timer <leave>
set gmrp timer <leaveall>
--------------------------------------------------------------------------------
set igmp leave-query-type <auto-mode | general-query | mac-gen-query>
set igmp querier <vlan-list> <value>
--------------------------------------------------------------------------------
```

```
set mls cef per-prefix-stats <enable|disable>
set mls nde version 1
set mls netflow-entry-create <enable|disable> <vlan-list>
set mls netflow-per-interface <enable|disable>
set mls rate <rate>
set mls statistics protocol <ip|ipnip|icmp|igmp|tcp|udp|<0..255>>
<dns|ftp|smtp|telnet|x|www|<1..65535>>
-------------------------------------------------------------------------------
set msfcautostate <enable|disable>
set msfcautostate exclude <port-list>
set msfcautostate track <enable|disable> <vlan>
set msfcautostate track <port-list>
-------------------------------------------------------------------------------
set ntp timezone [<hours> [<minutes>]]
set ntp timezone <zone_name>
set timezone <hours> [<minutes>]
set ntp key <public_keynum> trusted md4 <secret_keystring>
set ntp key <public_keynum> untrusted [md5 <secret_keystring>]
-------------------------------------------------------------------------------
set pbf
set pbf arp-inspection <name>
set pbf client <name> <ip_addr> <mac_addr> <vlan>
set pbf gw <name> <ip_addr> <ip_mask> <mac_addr> <vlan>
set pbf mac <mac_address>
set pbf vlan <vlan>
-------------------------------------------------------------------------------
set vmps config-file auto-save <enable|disable>
set vmps config-file <device:file_name>
set vmps downloadmethod rcp [<username>]
set vmps downloadmethod tftp
set vmps downloadserver < <hostname> | <ip_address> > [<filename>]
set vmps server reconfirminterval <1..120>
set vmps server retry <1..10>
set vmps server < <hostname> | <ip_address> > [primary]
set vmps state <disable|enable>
-------------------------------------------------------------------------------
set acllog ratelimit <1..9>
-------------------------------------------------------------------------------
set authentication login lockout <0 |<301..43200>>
[<$interface = console |telnet>]
set authentication enable lockout <0 |30..43200>> [<$interface = console |telnet>]
set authentication enable attempt <$num-attempts = 0 |3..10>
[<$interface = console |telnet>]
-------------------------------------------------------------------------------
set autoshut frequency <times>
set autoshut period <minutes>
-------------------------------------------------------------------------------
set default portstatus <enable|disable>
-------------------------------------------------------------------------------
set fan-tray-version <version>
-------------------------------------------------------------------------------
set filename-alias <name> <value>
-------------------------------------------------------------------------------
set garp timer all <join-value> <leave-value> <leaveall-value>
set garp timer join <time>
set garp timer <leave>
set garp timer <leaveall>
-------------------------------------------------------------------------------
set gvrp applicant <normal|active> <port-list>
set gvrp <enable|disable> [<port-list>]
set gvrp dynamic-vlan-creation <disable|enable>
set gvrp registration <fixed|forbidden|normal> <port-list>
set gvrp timer join <timer-value>
set gvrp timer leave <timer-value>
```

```
set gvrp timer leaveall <timer-value>
------------------------------------------------------------------------------
set image-verification [copy|boot|reset] <enable|disable>
------------------------------------------------------------------------------
set inlinpower defaultallocation <4000..15400>
set inlinepower notify-threshold <1..99> module <mod>
------------------------------------------------------------------------------
set macro ciscosmartports
------------------------------------------------------------------------------
set multicast router <port-list>
------------------------------------------------------------------------------
set pbf-map <name> <name>
------------------------------------------------------------------------------
set poll <enable|disable>
------------------------------------------------------------------------------
set rate-limit <l2port-security> <enable |disable>
set rate-limit <l2port-security> rate <rate>
set rate-limit <l2port-security> burst <rate>
------------------------------------------------------------------------------
set test diagfail-action <offline|ignore>
------------------------------------------------------------------------------
set port arp-inspection <port-list> drop-threshold <0-1000>
------------------------------------------------------------------------------
set port auxiliaryvlan <port-list> <vlan-list>
set port auxiliaryvlan <port-list> <vlan-list> cdpverify disable
set port auxiliaryvlan <port-list> <vlan-list> cdpverify enable
set port auxiliaryvlan <mod> <vlan-list>
set port auxiliaryvlan <mod> <vlan-list> cdpverify disable
set port auxiliaryvlan <mod> <vlan-list> cdpverify enable
------------------------------------------------------------------------------
set port channel all distribution <ip-vlan-session> <both |source |destination>
set port channel all mode off
set port channel <port-list> mode off
------------------------------------------------------------------------------
set port cops <port-list> roles {<role-name>}+
------------------------------------------------------------------------------
set port dhcp-snooping <port-list> source-guard <enable|disable>
------------------------------------------------------------------------------
set port dot1q-all-tagged <port-list> <enable|disable>
------------------------------------------------------------------------------
set port dot1x <port-list> port-control-direction <in|both>
set port dot1x <port-list> shutdown-timeout <disable|enable>
set port dot1x <port-list> <auth-fail-vlan | guest-vlan> <none | <vlan>>
set port dot1x <port-list> multiple-authentication <enable|disable>
set port dot1x <port-list> critical <enable|disable>
set port dot1x <port-list> test-eapol-capable
------------------------------------------------------------------------------
set port errordetection <port-list> <inerrors|rxcrc|txcrc> <enable|disable>
set port errdisable-timeout <port-list> <enable |disable>
------------------------------------------------------------------------------
set port <gmrp|gvrp> <port-list> <enable|disable>
------------------------------------------------------------------------------
set port lacp-channel <port-list> mode <off|on>
------------------------------------------------------------------------------
set port membership <port-list> <static|dynamic>
------------------------------------------------------------------------------
set port protocol <port-list> <group|ip|ipx> <auto|on|off>
------------------------------------------------------------------------------
set port rsvp <port-list> dsbm-election <enable|disable> [<128..255>]
------------------------------------------------------------------------------
set port security auto-configure <enable|disable>
------------------------------------------------------------------------------
set port macro <port-list> <ciscoswitch|ciscorouter> nativevlan <vlan> [allowedvlans
<vlan>]
```

```
set port macro <port-list> ciscosoftphone vlan <vlan> [allowedvlans <vlan>]
set port macro <port-list> ciscodesktop vlan <vlan>
set port macro <port-list> ciscoipphone vlan <vlan> [auxvlan
<none|dot1p|none|untagged|<vlan>]
--------------------------------------------------------------------------------
set port security-acl <port-list> <merge|port-based|vlan-based>
--------------------------------------------------------------------------------
set port voice interface < <mod>|<port-list> > enable
set port voice interface < <mod>|<port-list> > <disable|enable>
< <ip_addr/mask> | < <ip_addr> <mask> > >
vlan <vlan_num> gateway <ip_addr> tftp <ip_addr> dns <ip_addr> <domain_name>
set port voice interface < <mod>|<port-list> > <disable|enable>
< <ip_addr/mask> | < <ip_addr> <mask> > >
tftp <ip_addr> dns <ip_addr> <domain_name>
--------------------------------------------------------------------------------
set port vtp <port-list> <enable|disable>
--------------------------------------------------------------------------------
```

CHAPTER 13

# Troubleshooting the Network

Cisco E-DI provides diagnostic tools to allow you to troubleshoot the network by providing diagnostics on connectivity and performance. This chapter includes the following information:



## Diagnostics

Diagnostic tools allow you to diagnose potential connectivity issues in the network or for each individual device. Cisco E-DI provides the this diagnostics tool:

SNMP and Telnet/SSH connectivity check between Cisco E-DI and an NE.

You can also specify the credential set to be used for checking connectivity to the device.

Detailed information about connectivity and any problems encountered are displayed.

## Verifying Procedures

Cisco E-DI provides commands that can be used to verify that commands have been completed successfully. See Table 13-1.

*Table 13-1 Commands to Verify Procedures*

| Action | Command |
|---|---|
| To check that the SNMP server community string is set up correctly: | `[SVR:/server]# diag device server_ip` |
| To verify that the hostname has changed. | `[SVR:/server]# show running-config \| include hostname` |
| To verify that the IP address has changed. | `[SVR:/server]# show running-config` |
| To verify that the DNS server is configured. | `[SVR:/server]# show running-config` |
| To verify that the mail server is set up correctly. | `[SVR:/server]# sh run \| email username@cisco.com` |
| To verify that a script will run successfully. | `[NET:/network]# run file Script_path` |

*Table 13-1 Commands to Verify Procedures (continued)*

| Action | Command |
|---|---|
| To verify that a lock is created successfully. | `[SVR:/server]# show locks` |
| To verify that a lock is cleared successfully. | `[SVR:/server]# show locks` |
| To verify that the change-log contains performed operations on the server or network only if the priority of the task is greater than or equal to the defined change-log level setting. | `[SVR:/server]# show change-log` |
| To verify that the directory was created successfully, enter this command to show the contents of the current directory in the server file system. | `[SVR:/server]# dir` |
| To verify that the directory no longer exists in the server file system. | `[SVR:/server]# dir` |
| To verify that the file has been deleted from the server file system. | `[SVR:/server]# dir` |
| To verify that the directory has been copied. | `[SVR:/server]# dir` |
| To verify that the file has been saved to the destination directory. | `[SVR:/server]# dir` |
| To verify that changes have been saved. | `[SVR:/server]# show {startup-config \| running-config \| all} list-archives` |
| To verify that a label has been created.<br>The output should display the label if it is applicable to at least one device under the current context. | `[SVR:/server]# show labels details server_conf \| network_conf` |
| To verify that a configuration is restored. | `[SVR:/server]# show {startup-config \| running-config \| all} list-archives` |
| To verify the version on the device. | `[NET:/network]# show version` |
| To verify that the scheduled job has been created. | `[SVR:/server]# show job list` |
| To verify that the scheduled job has been deleted. | `[SVR:/server]# show job list` |

# Verifying Connectivity

You can verify connectivity:

- To a Specified Device
- To All Devices

## To a Specified Device

To verify connectivity to a specified device with a correct credential set using SNMP and Telnet, enter:

```
[NETWORK | SERVER]# diag device IP-Address [credential-set credential-set-name]
```

**Note** Optionally, a credential set to be used for connection can be provided.

## To All Devices

To perform SNMP and Telnet connectivity tests to all the devices currently managed by the Cisco E-DI server, enter:

```
[NET:/network]# diag connectivity [credential-set credential-set-name]
```

Optionally, a credential set to be used for connection can be provided.

**Note** The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

# Finding a Device or Host

Cisco E-DI provides commands to find managed devices and hosts in the network. See Table 13-2:

***Table 13-2 Commands to Find Devices in the Network***

| Action | Command |
|---|---|
| To find a managed device on the network.<br>This command is used to find the device based on the IP address or the MAC address or the name of the device. | `[SRV:/server\|NET:/network]# find devices {by-ip A.B.C.D \| by-mac H.H.H \| by-name name}` |
| To view the MAC address of the host and the switch it is connected to.<br>Sample find-host report:<br>`admin@edi-jms-1[SERVER]# find host by-mac 0002.55B7.6FA3`<br>`Host ip address = 172.25.86.71`<br>`Host mac address = 0002.55b7.6fa3`<br>`Connected to Switch = 172.25.86.109 on interface FastEthernet0/1 VlanId = 205` | `[SRV:/server\|NET:/network]# find host by-mac <H.H.H>` |
| To view the IP address of the host and the switch it is connected to.<br>Sample find-host report:<br>`admin@edi-jms-1[SERVER]# find host by-ip 172.25.86.171`<br>`Host ip address = 172.25.86.171`<br>`Host mac address = 0011.bce4.c540`<br>`nnected to Switch = 172.25.86.109 on interface FastEthernet0/1 VlanId = 205` | `[SRV:/server\|NET:/network]# find host by-ip <A.B.C.D>` |

CHAPTER 14

# Maintaining Cisco E-DI

Several tools are provided for Cisco E-DI server maintenance and troubleshooting:

- Maintenance Submode—The Cisco E-DI maintenance shell can be used to perform routine maintenance tasks such as installing patches or rebooting the Cisco E-DI server.
- Viewing Server Information—Administrators can view Cisco E-DI related information such as device-packages, clock, netstat, interfaces, and thread pools.
- Viewing License Information—Used to get information about the Cisco E-DI license.
- Viewing Security Features—Administrators can check the transport method, either SNMP Write or Telnet/SSH, and the credential set.

Cisco E-DI provides an aggregate log of all database transactions with their respective time stamps.

Cisco E-DI provides CLI commands to display:

- Linux process information
- Cisco E-DI thread pool sizes and pending tasks in the queue
- System memory usage
- System CPU usage

Cisco E-DI also generates internal statistics which can be output to a file.

## Viewing Server Information

Troubleshooting the server typically begins by looking at the server statistics and debug information. To enable administrators to view this information, Cisco E-DI provides options for the **show server** command. See Table 14-1.

***Table 14-1 Commands to View Server Information***

| Action | Command |
|---|---|
| To display installed Cisco E-DI device packages. | `[SRV:/server]# show server device-packages` |
| To print a list of event queues. | `[SRV:/server]# show server event-queues` |
| To display the server log information. | `[SRV:/server]# show server log [bookmark name \| log.1 \| log.2 \| log backup]` |

*Table 14-1 Commands to View Server Information (continued)*

| Action | Command |
|---|---|
| To display the known device types. | `[SRV:/server]# show server known-devices` |
| To print a list of all server software modules. | `[SRV:/server]# show server modules` |
| To display the server IP routing table. | `[SRV:/server]# show server routes` |
| To display the server running configuration for a module. | `[SRV:/server]# show server running-config module` |
| To display the server startup configuration. | `[SRV:/server]# show server startup-config` |
| To display the server statistics that include the aggregate count and the last occurrence for the following operations and events:<br>• Database backup, database restore.<br>• Discovery jobs.<br>• Inventory jobs run.<br>• SNMP—Traps sent, trap send failures.<br>• Syslog—Message send failures, messages sent, receiver decode errors, messages received but dropped, messages received.<br>• Server—Configuration change count, configuration load count, configuration save count.<br>• TFTP—Authentication failed requests, get requests, put requests.<br>• SNMP Traps—Traps received but dropped, known traps received, traps received, unknown traps received.<br>• Triggers—Failed action implementations, successful action implementations, successful pattern matches.<br>• XML API—Events sent, keep-alive requests received, XML requests received, XML responses sent out. | `[SRV:/server]# show server stats` |
| To print a list of thread pools. | `[SRV:/server]# show server thread-pools` |
| To print a list of all threads. | `[SRV:/server]# show server threads` |
| To show the server version. | `[SRV:/server]# show server version brief` |

In addition, administrators can use the **show line** command to view information on the sessions currently in use, including the userId, IP Address, connection mode and the uptime.

# Debug Logs

Debug logging can be enabled or altered or disabled on specific modules or on all the modules using the **debug** CLI command. When debug logging is enabled with a specific level, the messages that are generated by various modules at that level and above are logged into a log file.

Debug mode has the following levels of severity:

- fatal (5)
- error (4)
- warn (3)
- info (2)
- debug (1)

The debug log messages can be viewed using **show server log** command. The log output can be redirected to the terminal using the **terminal monitor** command. When the log file reaches the maximum size of 30MB, it is saved into a backup file.

These messages can be displayed on the terminal or logged to a file that you can access using the commands given in Table 14-2.

***Table 14-2 Commands to Debug Cisco E-DI***

| Action | Command |
|---|---|
| To set the debugging level for all the Cisco E-DI modules. | `[SVR:/server]# debug all level {debug \| error \| fatal \| info \| warn}` |
| To set the debugging level for a specific Cisco E-DI module to a pre-defined state. | `[SVR:/server]# debug module {module-name} level {debug \| error \| fatal \| info \| warn}` |
| To set a bookmark in the log file to facilitate retrieval of log messages between desired Cisco E-DI states. | `[SVR:/server]# debug bookmark {begin \| end} bookmark-name` |
| To show the contents of the log file for the specified bookmark. | `[SVR:/server]# show server log bookmark bookmark-name` |
| To print the logging messages to the terminal, | `[SVR:/server]# terminal monitor` |
| To clear the debug log.<br>See Table B-1 for details of the options available with this command. | `[SVR:/server]# clear debug-log` |

# Viewing License Information

Choose option **J** to display the license file status information. This command provides information including the license type (either permanent or demo), the MAC address of the Cisco E-DI server, and if a demo license is installed, the remaining days before the license expires.

# Viewing Security Features

Device authentication allows the administrator to choose between a centralized credential model (**non session based device authentication**) and a per user-session credential model (**session based device authentication**). Whichever mode is chosen is applied to all devices in the network. See Device Authentication for more details.

Table 14-3 details how to check the transport method, either SNMP Write or Telnet/SSH, and the credential set.

***Table 14-3 Commands to View Security Setup***

| Action | Command |
|---|---|
| To view the IP address of Cisco E-DI and the users' login ID. | `[SRV:/server]# show line` |
| To view the syslog messages on the devices. | `[NET:/network]# show events` |
| To check the status of management operations in Cisco E-DI | `[NET:/network]# show devices manageability` |

# Synchronizing Information

Cisco E-DI has the most current information about all of the devices in the network in its database. In case of any discrepancies found in the information when troubleshooting, you can synchronize the information between the server and the network.

Synchronization can be done in the foreground or the background.

The command for configuration synchronization is context sensitive.

Table 14-4 gives the commands to synchronize information in Cisco E-DI.

***Table 14-4 Commands to Synchronize Information***

| Action | Command |
|---|---|
| To synchronize the config-archives with the database for all offline and online devices, and server | `[NET:/network]# sync archives-with-db [all]` |
| To synchronize the file system with device. Synchronization can be done in the foreground or the background.<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | `[NET:/network]# sync filesystem {bg \| fg}` |
| To synchronize the startup and running config files with device. Synchronization can be done in the foreground or the background.<br>The behavior of this command changes when session based device authentication is enabled.<br>See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior. | `[NET:/network]# sync configuration {bg \| fg}` |
| To synchronize the asset inventory information. Synchronization can be done in the foreground or the background. | `[NET:/network]# sync asset {bg \| fg}` |

APPENDIX A

# Frequently Asked Questions

This section answers the Frequently Asked Questions (FAQs) on:

- Installation
- General
- Operational Data Modeler
- Device Configuration Manager
- Macro Command Manager
- Command Modeler
- Command Analyzer
- Command Translator

For the latest FAQs of Cisco Enhanced Device Interface, please check Cisco.com:

http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

## Installation

You can find the installation and setup usage details of Cisco Enhanced Device Interface in:

- *Installation and Setup Guide for Cisco Enhanced Device Interface 2.2, on Windows*
- *Installation and Setup Guide for Cisco Enhanced Device Interface 2.2, on Linux*

at: http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

Here are some FAQs related to Cisco E-DI installation:

**Q.** During the E-DI installation on Windows, I see that the postgress database setup has failed. What should I do?

**A.** Despite this message, continue with the installation. After completing the installation, uninstall E-DI. Stop security agent(s) if any are running, and then re-install E-DI. After successful installation, ensure that you start the security agents again.

**Q.** After starting E-DI server on Linux, database exceptions are being logged into /var/log/nemos.log. What should I do?

**A.** Stop and uninstall E-DI. Disable firewall settings if any, and install again. After installation, ensure that you enable the firewall settings again.

# General

You can find the complete usage details of Cisco Enhanced Device Interface in:

- *User Guide for Cisco Enhanced Device Interface*
- *Programmer's Guide for Cisco Enhanced Device Interface*

at: http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

The following are some Cisco E-DI FAQs:

**Q.** I am able to manage a device, but any device related operation fails.

**A.** Make sure that the firewall is disabled on the EDI server (use Linux commands **`iptables -L`** to list all the rules and **`iptables -F`** to clear on Linux).

If eth0 and eth1 are in different subnet than the device, then add the default gateway to EDI configuration using **`ip default-gateway`** *ip address*. Do not assign any ipv6 address on eth0 and eth1. EDI supports only eth0 and eth1, it will not accept the IP addresses that are allowed on any other interface.

**Q.** How can I find out what device packages are supported in this release?

**A.** To check the device packages that are supported in the current release of E-DI:

a. Start the E-DI service.

To do this, see the procedure in the Installation and Setup Guide for Cisco Enhanced Device Interface 2.2.

b. Using the Telnet console, log into Cisco E-DI server using admin credentials.

c. At the prompt, enter **`sh server device-packages`**.

The device packages are listed.

**Q.** I do not need all the device packages. How can I load only selected device packages? If I load only selected device packages, will it improve the performance of Cisco E-DI?

**A.** To load selected device packages:

a. Stop the E-DI service.

To do this, see the procedure in the Installation and Setup Guide for Cisco Enhanced Device Interface 2.2.

b. Go to *E-DI Install Location*/Cisco EDI/edi/dist/devpackages directory.

This directory contains *.jdp files each for a given device family.

c. Rename the device packages that are not required, with the extension **`.old,`** for example.

d. Start the E-DI service.

To do this, see the procedure in the Installation and Setup Guide for Cisco Enhanced Device Interface 2.2.

Yes, this will enhance the performance of Cisco E-DI in cases where you do not need all the device packages.

**Q.** If I need to download device packages from the IDU/Service Pack releases, where do I go?

**A.** You can download the device packages from: http://www.cisco.com/cgi-bin/tablebuild.pl/E-DI-2.0. To get the required device package:

a. Check whether the device package is available at this URL: http://www.cisco.com/cgi-bin/tablebuild.pl/E-DI-2.0.

b. If it is present, download the device package.

   You need to have your Cisco.com user login to download these packages.

c. After downloading the device packages, copy them to the *E-DI Install Location*/Cisco EDI/edi/dist/devpackages directory.

# Operational Data Modeler

You can find the complete usage details of Operational Data Modeler in *Programmer's Guide for Cisco Enhanced Device Interface*, at:
http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

The following are the FAQs for Operational Data Modeler:

**Q.** Is ordering of elements important in a Spec file?

**A.** Yes, ordering of elements is important in a Spec file. The elements should be in the same order as the order in which they appear in CLI, from left to right and top to bottom.

**Q.** I am not sure where I am allowed to use **`dynamic`** option of **`<Container>`**.

**A.** Yes, you can use the **`dynamic`** option for looping data structures where multiple instances are possible for a particular data model. For example, in the output of **`show interfaces`** or **`show interface stats`** IOS commands, the data model will be repeated for each interface instance. The structure of data (interface details) will remain same.

Only the values for the data elements (that is, the properties) will vary. Instead of repeating the same data model multiple times (where the number of repetition is also unknown), you can define a single data model and mark it **`dynamic`** for repeated occurrences of the same model. This is a looped data model, where the loop will be run for each instance.

**Q.** Are **`distance, length, start`** and **`end`** valid for both **`<Property>`** and **`<Header>`**?

**A.** **`Start`** and **`end`** are valid only for the **`<Header>`** tag. These **`start`** and **`end`** tags are used for specifying spatial information (that is, the starting and ending positions) of a particular column in tabular data. **`distance`** and **`length`** attributes are applicable only for the **`<Property>`** tag.

**Q.** Are **`<Option>`** elements valid within **`<Header>`** elements?

**A.** Yes, **`<Option>`** elements are applicable to both properties (**`<Property>`**) as well as column headers (**`<Header>`**).

**Q.** How do I decide on a `length` value in the `<Property>` tag?

**A.** The `length` value indicates the maximum words that can be combined to form the value. For example, in the CLI line: `"Compiled Fri 22-Dec-06 03:12 by prod_rel_team",` the keyword `Compiled` will have the date value which will always consist of 3 words `"Fri 22-Dec-06 03:12"` (day/date/time).

In this case `length` can have the value as 3 since the value will always consist of 3 words. If the value is -1, it means that all the words till the end of the line or the start of the line, depending upon the direction of value with respect to keyword (whether value is in right or left of keyword specified), are combined to form a value.

# Device Configuration Manager

You can find the complete usage details of Device Configuration Manager in *User Guide for Cisco Enhanced Device Interface*, at:
http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

Device Configuration Manager is also known as Config Manager.

The following are the FAQs for Device Configuration Manager (DCM):

**Q.** In the DCM Editor, syntax coloring does not appear. At times it appears to be incomplete. What should I do?

**A.** While you are working on the Editors, if the syntax coloring does not appear, or is incomplete, you should refresh the Editor by right-clicking on the editor and selecting **Refresh Editor**, from the context menu.

**Q.** I cannot save the contents of the Editor. Why?

**A.** By default, you will not be able to save the contents of the Editor, unless you have made some changes to the content. If you want to save the contents, press the Enter key. Then right-click and select **Save** from the context menu. Your contents will be saved.

**Q.** How can one check the syntax of a configuration?

**A.** Open the command Editor in Device Configuration Manager and paste the contents of the configuration. Select the device type and OS version. The command Editor will highlight the content with the syntax colors. Any invalid configuration will be shown in red.

**Q.** How can Device Configuration Manager (DCM) be used for OS migration/upgradation?

**A.** One of the main tasks for the OS migration is to validate the current running configuration against the new OS Version.

The command Editor of DCM can be of help in this regard:

a. Open the command Editor and copy the current running configuration to this editor.

b. Select the target (new) DeviceType and OS Version from the version selector combo boxes.

The editor will highlight the contents with appropriate syntax colors. Any invalid configuration will be shown in red.

# Macro Command Manager

You can find the complete usage details of Macro Command Manager in *User Guide for Cisco Enhanced Device Interface*, at:
http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

The following are the FAQs for Macro Command Manager:

**Q.** The macros I created using the Macro Command Manager GUI were lost after the E-DI server stopped.

**A.** After the GUI changes are done, ensure that you perform a **Save Macro Changes** operation. Unless your changes are saved, they are not updated to the server database. If the server restarts, these changes are lost.

**Q.** Deploy macro command generates a message that the deploy was successful although the command was not applied to the device. Why does this happen?

**A.** The deploy macro command creates a temp file and uploads the file to the device using TFTP. A temporary file will be generated in the server/temp folder. Check the contents of the file to see if they are valid on the device.

# Command Modeler

You can find the complete usage details of Command Modeler in *Programmer's Guide for Cisco Enhanced Device Interface*, at:
http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

The following are the FAQs for Command Modeler:

**Q.** What are the jar files needed for compiling the code generated by EDI?

**A.** nemo.jar, cliparser.jar, nodetypes.jar, log4j-1.2.8.jar, javolution.jar are needed for compilation. All these jar files are present under subfolders in the E-DI install directory.

**Q.** What is the use of toXml () method provided in the generated class?

**A.** The toXml () method generates the xml transformation of the CLI. This can be used along with the XML Programatic interface.

# Command Analyzer

You can find the complete usage details of Command Analyzer in *Programmer's Guide for Cisco Enhanced Device Interface*, at:
http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

The following are the FAQs for Command Analyzer:

**Q.** The required device family is not available in the list of devices that can be selected for the generation of report. Why is this?

**A.** The device package for that particular device may not be present in the device package directory specified in the Setup wizard. To get the required device package:

a. Check whether the device package is available at this URL: http://www.cisco.com/cgi-bin/tablebuild.pl/E-DI-2.0.

b. If it is present, download the device package. You need to have your Cisco.com user login to download these packages.

c. After downloading the device packages, copy them to the *E-DI Install Location*\Cisco EDI\edi\dist\devpackages directory.

d. Re-enter the details in the Setup Wizard and submit it.

**Q.** How do I save the generated report?

**A.** After you have generated either the Commands Report or the Commands Comparison Report, use the **Tools > Export to PDF** option to save the generated report as PDF file in the file system.

**Q.** What do the colors in the report indicate?

**A.** To know more about the color indicators in the report, click on the hyperlink labeled **Click here for the legends**. The legends or colors being used in the report are described here.

# Command Translator

You can find the complete usage details of Command Translator in *User Guide for Cisco Enhanced Device Interface*, at:
http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

The following are the FAQs for Command Translator:

**Q.** The Command Translator reports translation errors for some of the lines in the converted Cisco IOS configuration file. How can I resolve these?

**A.** Some cases require more information than the configuration file provides. For example, many QoS configuration commands have dependencies on ACLs or policies. If these commands are not included, the tool cannot provide a complete translation.

In other cases, there is no Cisco IOS equivalent command, as is the case with commands related to the CatOS sc0 interface.

Sometimes, a command is intentionally not translated in order to require you to make a conscious configuration for a critical setting, such as the AAA services.

For a list of CatOS commands that are not translated in this release, see the topic Untranslated CatOS Commands, in the section Translating Commands Using Command Translator, of the *User Guide for Cisco Enhanced Device Interface* at:
http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html

**Q.** Why does the Command Translator translate both the **set port name** and the **set port description** CatOS commands into the port description Cisco IOS interface configuration command?

**A.** Cisco IOS does not have an equivalent to the CatOS **set port name**, but the **set port name** command is often used as a description. Therefore this command needs to translate to Cisco IOS. The dilemma occurs when both the **set port name** and the **set port description** CatOS commands are used, because only one command can be used in the Cisco IOS configuration. Although both commands translate into the Cisco IOS translated configuration, you must delete whichever one is not needed.

**Q.** Why are my sc0 interface commands not translated?

**A.** Cisco IOS does not implement an sc0 interface. This is an architectural difference between CatOS and Cisco IOS. In Cisco IOS, any interface can be configured as a management interface.

**Q.** Why are my banner-related commands not translated?

**A.** The translation of the CatOS Banner into the Cisco IOS Banner is under consideration for a future release of the tool.

**Q.** Why are my AAA-related commands not translated?

**A.** These commands are critical in order to maintain access to the switch, therefore it is important to try to configure these parameters so that access to the switch is not blocked.

**Q.** I use a Hybrid operating system with both CatOS and Cisco IOS on the MSFC. Can the tool integrate my MSFC Cisco IOS configuration as well?

**A.** No, the tool cannot integrate the MSFC configuration into the translated CatOS configuration. Most of the MSFC Cisco IOS commands convert as-is into a new Cisco IOS switch configuration.

**Q.** Can I use the output from a show run for the CatOS input file or does this have to be a full copy of the configuration file downloaded from the switch?

**A.** You can use the **show run** output.

**Q.** Do I have to provide a show module output for every conversion?

**A.** The **show module** output is optional. The **show module** output only assists with certain **set QoS** commands.

**Q.** What are the minimum software versions for CatOS and Cisco IOS supported by the tool?

**A.** The Command Translator supports CatOS version 8.5.1 and earlier. The translated Cisco IOS configuration file can be based on Cisco IOS Software Release 12.2.18SXF3 or Cisco IOS Software Release 12.2.18.SXF5.

**Q.** Is there a list or database of known CatOS commands that do not translate into a Cisco IOS equivalent?

Yes. For a list of CatOS commands that are not translated in this release, see the topic Untranslated CatOS Commands, in the section Translating Commands Using Command Translator, of the *User Guide for Cisco Enhanced Device Interface* at: http://www.cisco.com/en/US/products/ps6456/tsd_products_support_series_home.html.

**Q.** The required device family is not available in the list of devices that can be selected for the creation of unified model. Why is this?

**A.** Device package for that particular device is not present in the device package directory specified in the Setup wizard. To get the required device package:

a. Check whether the device package is available at this URL: http://www.cisco.com/cgi-bin/tablebuild.pl/E-DI-2.0.

b. If it is present, download the device package. You need to have your Cisco.com user login to download these packages.

c. After downloading the device packages, copy them to the *E-DI Install Location*\Cisco EDI\edi\dist\devpackages directory.

d. Re-enter the details in the Setup Wizard and submit it.

**Q.** Where are the generated Java files stored?

**A.** The generated Java files are stored in the Code Output Directory specified in the Setup Wizard.

**Q.** How do I enter the package name for the Java code generated by Command Modeler?

**A.** During generation of code, you are prompted to enter a package name for the Java code. In the current release, there is no support for a default package.

APPENDIX B

# Cisco E-DI Commands and Associated Privileges

This appendix lists all the commands available in Cisco E-DI, and identifies the privileges associated with each command.

You can enter part of a command and press the **Tab** key to complete the command.

Enter **?** after a command to view the options available with that command, and a brief explanation of its use.

The behavior of some commands changes when session based device authentication is enabled. These commands are identified with an asterisk (*) in Table B-1.

See Using Session Based Device Authentication, page 2-8 for a full explanation of the command behavior.

***Table B-1 Cisco E-DI Commands and Associated Privileges***

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| **No/Yes:**: Server mode/Network mode permissions. For example: No/Yes: Not allowed to implement in server mode, but allowed in network mode. | | | | |
| **No:** You are not allowed to implement the command in both server and network mode | | | | |
| **Yes:** You are allowed to implement the command in both server and network mode | | | | |
| aaa server radius \| tacacs A.B.C.D key encryption-level key-value <cr> | Yes | No | No | No |
| cd <cr> | Yes | Yes | Yes | No |
| cd DIRNAME <cr> | Yes | Yes | Yes | No |
| clear alarms <cr> | Yes | No/Yes | No | No |
| clear alarms condition ALARM-CONDITION <cr> | Yes | No/Yes | No | No |
| clear alarms device A.B.C.D <cr> | Yes | No/Yes | No | No |
| clear alarms device A.B.C.D condition ALARM-CONDITION <cr> | Yes | No/Yes | No | No |
| clear alarms group GROUPNAME <cr> | Yes | No/Yes | No | No |
| clear alarms group GROUPNAME condition ALARM-CONDITION <cr> | Yes | No/Yes | No | No |
| clear alarms id <1-100000> <cr> | Yes | No/Yes | No | No |
| clear alarms network <cr> | Yes | No/Yes | No | No |
| clear alarms server <cr> | Yes | No/Yes | No | No |
| clear change-log <cr> | Yes | No | No | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| clear change-log older-than days <1-240> <cr> | Yes | No | No | No |
| clear change-log older-than hours <1-240> <cr> | Yes | No | No | No |
| clear cmd-err-count <cr> | Yes | Yes | Yes | Yes |
| clear config-archives all <cr> | Yes | No/Yes | No | No |
| clear config-archives all older-than days <1-1000> <cr> | Yes | No/Yes | No | No |
| clear config-archives all older-than time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| clear config-archives all older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| clear config-archives all older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D all <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D all older-than days <1-1000> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D all older-than time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D all older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D all older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D running-config <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D running-config older-than days <1-1000> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D running-config older-than time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D running-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D running-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D startup-config <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D startup-config older-than days <1-1000> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D startup-config older-than time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D startup-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| clear config-archives device A.B.C.D startup-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| clear config-archives running-config <cr> | Yes | No/Yes | No | No |
| clear config-archives running-config older-than days <1-1000> <cr> | Yes | No/Yes | No | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| clear config-archives running-config older-than time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| clear config-archives running-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| clear config-archives running-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| clear config-archives startup-config <cr> | Yes | No/Yes | No | No |
| clear config-archives startup-config older-than days <1-1000> <cr> | Yes | No/Yes | No | No |
| clear config-archives startup-config older-than time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| clear config-archives startup-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| clear config-archives startup-config older-than time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| clear debug-log <cr> | Yes | Yes | No | No |
| clear devices <cr> | Yes | No | No | No |
| clear devices A.B.C.D <cr> | Yes | No | No | No |
| clear devices all <cr> | Yes | No | No | No |
| clear devices ip-range A.B.C.D A.B.C.D <cr> | Yes | No | No | No |
| clear discovery devices-discovered <cr> | Yes | No | No | No |
| clear discovery history <cr> | Yes | No | No | No |
| clear events <cr> | Yes | No/Yes | No | No |
| clear events all network <cr> | Yes | No/Yes | No | No |
| clear events all server <cr> | Yes | No/Yes | No | No |
| clear events older-than days <1-240> <cr> | Yes | No/Yes | No | No |
| clear events older-than hours <1-240> <cr> | Yes | No/Yes | No | No |
| clear ip-aliases [all \| ip-range] <cr> | Yes | No | No | No |
| clear label all <cr> | Yes | No/Yes | No | No |
| clear label RESTORE-LABEL <cr> | Yes | No/Yes | No | No |
| clear line <0-16> <cr> | Yes | No | No | No |
| clear line all <cr> | Yes | No | No | No |
| clear lock <cr> | Yes | Yes | No | No |
| clear lock override <cr> | Yes | No | No | No |
| clear report availability <cr> | Yes | No | No | No |
| clear report upgrade-log <cr> | Yes | No | No | No |
| clear server log <cr> | Yes | No | No | No |
| clear server stats <cr> | Yes | No | No | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| clear status connections <cr> | Yes | Yes | No | No |
| clear status connections all <cr> | Yes | Yes | No | No |
| configure <cr> | Yes | No/Yes | No | No |
| configure setup <cr> * | Yes | Yes | Yes | Yes |
| configure terminal <cr> | Yes | No | No | No |
| connect exec-mode <cr> [netexec] * | Yes | Yes | No | No |
| copy FILENAME FILENAME <cr> * | Yes | Yes | No | No |
| copy FILENAME nodename://file <cr> | Yes | Yes | No | No |
| copy FILENAME tftp://A.B.C.D/file <cr> | Yes | Yes | No | No |
| copy nodename://file FILENAME <cr> | Yes | Yes | No | No |
| copy nodename://file nodename://file <cr> | Yes | Yes | No | No |
| copy nodename://file tftp://A.B.C.D/file <cr> | Yes | Yes | No | No |
| copy tftp://A.B.C.D/file FILENAME <cr> | Yes | Yes | No | No |
| copy tftp://A.B.C.D/file nodename://file <cr> | Yes | Yes | No | No |
| database backup FILENAME <cr> | Yes | No | No | No |
| database restore FILENAME <cr> | Yes | No | No | No |
| database backup ftp <host> FILENAME <cr> | Yes | No | No | No |
| database restore ftp <host> FILENAME <cr> | Yes | No | No | No |
| debug all <no> | Yes | Yes | Yes | No |
| debug all level debug <cr> | Yes | Yes | Yes | No |
| debug all level error <cr> | Yes | Yes | Yes | No |
| debug all level fatal <cr> | Yes | Yes | Yes | No |
| debug all level info <cr> | Yes | Yes | Yes | No |
| debug all level warn <cr> | Yes | Yes | Yes | No |
| debug bookmark begin WORD <cr> | Yes | Yes | Yes | No |
| debug bookmark end WORD <cr> | Yes | Yes | Yes | No |
| debug module MODULE <no> | Yes | Yes | Yes | No |
| debug module MODULE level debug <cr> | Yes | Yes | Yes | No |
| debug module MODULE level error <cr> | Yes | Yes | Yes | No |
| debug module MODULE level fatal <cr> | Yes | Yes | Yes | No |
| debug module MODULE level info <cr> | Yes | Yes | Yes | No |
| debug module MODULE level warn <cr> | Yes | Yes | Yes | No |
| delete /force /recursive FILENAME <cr> | Yes | No | No | No |
| delete /force FILENAME <cr> | Yes | No | No | No |
| delete /recursive /force FILENAME <cr> | Yes | No | No | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| delete /recursive FILENAME <cr> | Yes | No | No | No |
| delete FILENAME <cr> | Yes | No | No | No |
| device-auth session based <cr> | Yes | No | No | No |
| diag connectivity <cr> * | Yes | Yes | Yes | No |
| diag connectivity credential-set CREDENTIAL-SET <cr> | Yes | Yes | Yes | No |
| diag device A.B.C.D <cr> | Yes | Yes | Yes | No |
| diag device A.B.C.D credential-set CREDENTIAL-SET <cr> | Yes | Yes | Yes | No |
| diff FILENAME FILENAME <cr> | Yes | Yes | Yes | No |
| diff-config PARAMETER-TYPE FILENAME FILENAME <cr> | Yes | Yes | Yes | No |
| diff-config PARAMETER-TYPE FILENAME FILENAME rollback-script <cr> | Yes | Yes | Yes | No |
| dir <cr> | Yes | Yes | Yes | No |
| dir FILENAME <cr> | Yes | Yes | Yes | No |
| discover cdp A.B.C.D <cr> | Yes | No | No | No |
| discover cdp A.B.C.D hopcount <0-20> <cr> | Yes | No | No | No |
| discover cdp A.B.C.D hopcount <0-20> ignore <cr> | Yes | No | No | No |
| discover snmp-scan A.B.C.D A.B.C.D <cr> | Yes | No | No | No |
| discovery use-mgmt-ip-address <cr> | Yes | No | No | No |
| discovery use-mgmt-ip-binding <cr> | Yes | No | No | No |
| do-snmp get | Yes | Yes | No | No |
| do-snmp oid-lookup | Yes | Yes | No | No |
| do-snmp print mib-list | Yes | Yes | No | No |
| do-snmp set | Yes | Yes | No | No |
| do-snmp walk | Yes | Yes | No | No |
| downloadWORD FILENAME <cr> | Yes | Yes | No | No |
| echo WORD <cr> | Yes | Yes | Yes | No |
| edit FILENAME <cr> | Yes | No | No | No |
| erase server startup-config <cr> | Yes | No | No | No |
| exec-cmd WORD <cr> * | Yes | Yes | No | No |
| find devices by-ip A.B.C.D <cr> | Yes | Yes | Yes | No |
| find devices by-mac H.H.H <cr> | Yes | Yes | Yes | No |
| find devices by-name WORD <cr> | Yes | Yes | Yes | No |
| find host by-ip <A.B.C.D> <cr> | Yes | Yes | Yes | No |
| find host by-mac <H.H.H> <cr> | Yes | Yes | Yes | No |
| generate xsd | Yes | No | No | No |
| iferror WORD <cr> | Yes | Yes | Yes | Yes |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| ifok WORD <cr> | Yes | Yes | Yes | Yes |
| import devices from-discovered-list <cr> | Yes | No | No | No |
| import devices from-discovered-list all <cr> | Yes | No | No | No |
| import devices from-seed-file <filename> | Yes | No | No | No |
| inventory <cr> * | Yes | Yes | No | No |
| inventory group GROUPNAME <cr> | Yes | Yes | No | No |
| ip-alias device\|group <A.B.C.D\|name> sub-interface <A.B.C.D> netmask <A.B.C.D> <cr> | Yes | No | No | No |
| label WORD <cr> | Yes | No/Yes | No | No |
| label WORD descr WORD <cr> | Yes | No/Yes | No | No |
| label WORD RESTORE-FILE RESTORE-FILE <cr> | Yes | No/Yes | No | No |
| label WORD RESTORE-FILE RESTORE-FILE descr WORD <cr> | Yes | No/Yes | No | No |
| label WORD time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| label WORD time <2003-2020> <1-12> <1-31> descr WORD <cr> | Yes | No/Yes | No | No |
| label WORD time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| label WORD time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> descr WORD <cr> | Yes | No/Yes | No | No |
| label WORD time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| label WORD time <2003-2020> <1-12> <1-31> hh:mm:ss descr WORD <cr> | Yes | No/Yes | No | No |
| load-config <cr> | Yes | No | No | No |
| load-config FILENAME <cr> | Yes | No | No | No |
| lock reason WORD <cr> | Yes | No/Yes | No | No |
| lock reason WORD type local <cr> | Yes | No/Yes | No | No |
| lock reason WORD type remote <cr> | Yes | No/Yes | No | No |
| login <cr> * | Yes | Yes | Yes | Yes |
| logout <cr> | Yes | Yes | Yes | Yes |
| mkdir FILENAME <cr> | Yes | Yes | No | No |
| more FILENAME <cr> * | Yes | Yes | Yes | No |
| network <cr> | Yes | Yes | Yes | No |
| network A.B.C.D <cr> | Yes | Yes | Yes | No |
| network A.B.C.D dnsname Hostname or A.B.C.D <cr> | Yes | Yes | Yes | No |
| network A.B.C.D dnsname Hostname or A.B.C.D group GROUPNAME <cr> | Yes | Yes | Yes | No |
| network A.B.C.D group GROUPNAME <cr> | Yes | Yes | Yes | No |
| network A.B.C.D group GROUPNAME dnsname Hostname or A.B.C.D <cr> | Yes | Yes | Yes | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| network dnsname Hostname or A.B.C.D <cr> | Yes | Yes | Yes | No |
| network dnsname Hostname or A.B.C.D A.B.C.D <cr> | Yes | Yes | Yes | No |
| network dnsname Hostname or A.B.C.D A.B.C.D group GROUPNAME <cr> | Yes | Yes | Yes | No |
| network dnsname Hostname or A.B.C.D group GROUPNAME <cr> | Yes | Yes | Yes | No |
| network dnsname Hostname or A.B.C.D group GROUPNAME A.B.C.D <cr> | Yes | Yes | Yes | No |
| network group GROUPNAME <cr> | Yes | Yes | Yes | No |
| network group GROUPNAME A.B.C.D <cr> | Yes | Yes | Yes | No |
| network group GROUPNAME A.B.C.D dnsname Hostname or A.B.C.D <cr> | Yes | Yes | Yes | No |
| network group GROUPNAME dnsname Hostname or A.B.C.D <cr> | Yes | Yes | Yes | No |
| network group GROUPNAME dnsname Hostname or A.B.C.D A.B.C.D <cr> | Yes | Yes | Yes | No |
| network hostname WORD <cr> | Yes | Yes | Yes | No |
| nslookup WORD <cr> | Yes | Yes | Yes | Yes |
| perl FILENAME <cr> | Yes | Yes | No | No |
| perl FILENAME WORD <cr> | Yes | Yes | Yes | No |
| poll device A.B.C.D <cr> | Yes | Yes | No | No |
| poll-interval <poll-frequency> <cr> | Yes | No | No | No |
| pwd <cr> * | Yes | Yes | Yes | No |
| raise alarm ALARM-CONDITION WORD <cr> | Yes | Yes | Yes | Yes |
| raise alarm ALARM-CONDITION WORD WORD <cr> | Yes | Yes | Yes | Yes |
| relay-agent syslog A.B.C.D <cr> | Yes | No | No | No |
| reload device A.B.C.D <cr> * | Yes | Yes | No | No |
| rename WORD WORD <cr> | Yes | No | No | No |
| restore label RESTORE-LABEL <cr> | Yes | No/Yes | No | No |
| restore RESTORE-FILE RESTORE-FILE <cr> | Yes | No/Yes | No | No |
| restore time <2003-2020> <1-12> <1-31> <cr> | Yes | No/Yes | No | No |
| restore time <2003-2020> <1-12> <1-31> hh:mm:ss <0-999> <cr> | Yes | No/Yes | No | No |
| restore time <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | No/Yes | No | No |
| rmdir FILENAME <cr> | Yes | No | No | No |
| run file FILENAME <cr> | Yes | Yes | Yes | Yes |
| server <cr> | Yes | Yes | Yes | Yes |
| server configure <cr> | Yes | No | No | No |
| server maintenance <cr> [server-maint] | Yes | No | No | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| service arp <cr> | Yes | No | No | No |
| service config <cr> | Yes | No | No | No |
| service filesystem <cr> | Yes | No | No | No |
| service inventory <cr> | Yes | No | No | No |
| service mac-address-table <cr> | Yes | No | No | No |
| service performance <cr> | Yes | No | No | No |
| service statuspoller <cr> | Yes | No | No | No |
| service stp <cr> | Yes | No | No | No |
| service vtp <cr> | Yes | No | No | No |
| setup-wizard setup-server <cr> | Yes | No | No | No |
| show alarms <cr> | Yes | Yes | Yes | No |
| show alarms all <cr> | Yes | Yes | Yes | No |
| show alarms all condition ALARM-CONDITION <cr> | Yes | Yes | Yes | No |
| show alarms all details <cr> | Yes | Yes | Yes | No |
| show alarms all filter WORD <cr> | Yes | Yes | Yes | No |
| show alarms all severity SEVERITY <cr> | Yes | Yes | Yes | No |
| show alarms condition ALARM-CONDITION <cr> | Yes | Yes | Yes | No |
| show alarms details <cr> | Yes | Yes | Yes | No |
| show alarms device A.B.C.D <cr> | Yes | Yes | Yes | No |
| show alarms device A.B.C.D all <cr> | Yes | Yes | Yes | No |
| show alarms device A.B.C.D all details <cr> | Yes | Yes | Yes | No |
| show alarms device A.B.C.D condition ALARM-CONDITION <cr> | Yes | Yes | Yes | No |
| show alarms device A.B.C.D condition ALARM-CONDITION details <cr> | Yes | Yes | Yes | No |
| show alarms device A.B.C.D details <cr> | Yes | Yes | Yes | No |
| show alarms device A.B.C.D severity SEVERITY <cr> | Yes | Yes | Yes | No |
| show alarms filter WORD <cr> | Yes | Yes | Yes | No |
| show alarms group GROUPNAME <cr> | Yes | Yes | Yes | No |
| show alarms group GROUPNAME all <cr> | Yes | Yes | Yes | No |
| show alarms group GROUPNAME all details <cr> | Yes | Yes | Yes | No |
| show alarms group GROUPNAME condition ALARM-CONDITION <cr> | Yes | Yes | Yes | No |
| show alarms group GROUPNAME condition ALARM-CONDITION details <cr> | Yes | Yes | Yes | No |
| show alarms group GROUPNAME details <cr> | Yes | Yes | Yes | No |
| show alarms group GROUPNAME severity SEVERITY <cr> | Yes | Yes | Yes | No |
| show alarms id <1-100000> <cr> | Yes | Yes | Yes | No |
| show alarms network <cr> | Yes | Yes | Yes | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| show alarms server <cr> | Yes | Yes | Yes | No |
| show alarms severity SEVERITY <cr> | Yes | Yes | Yes | No |
| show arp <cr> | Yes | Yes | Yes | No |
| show arp ipaddress <A.B.C.D> <cr> | Yes | Yes | Yes | No |
| show arp macaddress <H.H.H> <cr> | Yes | Yes | Yes | No |
| show mac-address-table <cr> | Yes | Yes | Yes | No |
| show asset all <cr> | Yes | Yes | Yes | No |
| show asset cards <cr> | Yes | Yes | Yes | No |
| show asset chassis <cr> | Yes | Yes | Yes | No |
| show asset fans <cr> | Yes | Yes | Yes | No |
| show asset ports <cr> | Yes | Yes | Yes | No |
| show asset power-supply <cr> | Yes | Yes | Yes | No |
| show asset slots <cr> | Yes | Yes | Yes | No |
| show cdp neighbors <cr> | Yes | Yes | Yes | No |
| show change-log <cr> | Yes | Yes | Yes | No |
| show change-log last <1-100000> <cr> | Yes | Yes | Yes | No |
| show change-log WORD <cr> | Yes | Yes | Yes | No |
| show change-log WORD last <1-100000> <cr> | Yes | Yes | Yes | No |
| show cmd-err-count <cr> | Yes | Yes | Yes | No |
| show debug-log <cr> | Yes | Yes | Yes | No |
| show devices <cr> | Yes | Yes | Yes | No |
| show devices capabilities <cr> | Yes | Yes | Yes | No |
| show devices detail <cr> | Yes | Yes | Yes | No |
| show devices group GROUPNAME <cr> | Yes | Yes | Yes | No |
| show devices manageability <cr> | Yes | Yes | Yes | No |
| show discovery devices-discovered <cr> | Yes | Yes | Yes | No |
| show discovery devices-discovered mgmt-ip-binding <cr> | Yes | Yes | Yes | No |
| show discovery devices-discovered WORD <cr> | Yes | Yes | Yes | No |
| show discovery history <cr> | Yes | Yes | Yes | No |
| show discovery history WORD <cr> | Yes | Yes | Yes | No |
| show discovery task-history <cr> | Yes | Yes | Yes | No |
| show events <cr> | Yes | Yes | Yes | No |
| show events between <2003-2020> <1-12> <1-31> <cr> | Yes | Yes | Yes | No |
| show events between <2003-2020> <1-12> <1-31> hh:mm:ss <2003-2020> <1-12> <1-31> <cr> | Yes | Yes | Yes | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| show events between <2003-2020> <1-12> <1-31> hh:mm:ss <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | Yes | Yes | No |
| show events between <2003-2020> <1-12> <1-31> hh:mm:ss <2003-2020> <1-12> <1-31> hh:mm:ss raw-format <cr> | Yes | Yes | Yes | No |
| show events between <2003-2020> <1-12> <1-31> hh:mm:ss <2003-2020> <1-12> <1-31> raw-format <cr> | Yes | Yes | Yes | No |
| show events between <2003-2020> <1-12> <1-31> hh:mm:ss <cr> | Yes | Yes | Yes | No |
| show events between <2003-2020> <1-12> <1-31> hh:mm:ss raw-format <cr> | Yes | Yes | Yes | No |
| show events between <2003-2020> <1-12> <1-31> raw-format <cr> | Yes | Yes | Yes | No |
| show events device A.B.C.D <cr> | Yes | Yes | Yes | No |
| show events device A.B.C.D last <1-100000> <cr> | Yes | Yes | Yes | No |
| show events device A.B.C.D raw-format <cr> | Yes | Yes | Yes | No |
| show events device A.B.C.D raw-format last <1-100000> <cr> | Yes | Yes | Yes | No |
| show events device A.B.C.D summary <cr> | Yes | Yes | Yes | No |
| show events filter WORD <cr> | Yes | Yes | Yes | No |
| show events group GROUPNAME <cr> | Yes | Yes | Yes | No |
| show events group GROUPNAME last <1-100000> <cr> | Yes | Yes | Yes | No |
| show events group GROUPNAME raw-format <cr> | Yes | Yes | Yes | No |
| show events group GROUPNAME raw-format last <1-100000> <cr> | Yes | Yes | Yes | No |
| show events group GROUPNAME summary <cr> | Yes | Yes | Yes | No |
| show events last <1-100000> <cr> | Yes | Yes | Yes | No |
| show events last <1-100000> summary <cr> | Yes | Yes | Yes | No |
| show events raw-format <cr> | Yes | Yes | Yes | No |
| show events raw-format filter WORD <cr> | Yes | Yes | Yes | No |
| show events raw-format last <1-100000> <cr> | Yes | Yes | Yes | No |
| show events summary <cr> | Yes | Yes | Yes | No |
| show groups <cr> | Yes | Yes | Yes | No |
| show interfaces <cr> | Yes | Yes | Yes | No |
| show interfaces IF-GROUP <cr> | Yes | Yes | Yes | No |
| show interfaces IF-GROUP device A.B.C.D <cr> | Yes | Yes | Yes | No |
| show interfaces IF-GROUP group GROUPNAME <cr> | Yes | Yes | Yes | No |
| show ip interface brief <cr> | Yes | Yes | Yes | No |
| show job details WORD <cr> | Yes | Yes | Yes | No |
| show job details WORD logs <cr> | Yes | Yes | Yes | No |
| show job details WORD logs latest <cr> | Yes | Yes | Yes | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| show job list <cr> | Yes | Yes | Yes | No |
| show labels <cr> | Yes | Yes | Yes | No |
| show labels detail <cr> | Yes | Yes | Yes | No |
| show labels detail RESTORE-LABEL <cr> | Yes | Yes | Yes | No |
| show line <0-16> <cr> | Yes | Yes | Yes | No |
| show line <cr> | Yes | Yes | Yes | No |
| show line all <cr> | Yes | Yes | Yes | No |
| show locks <cr> | Yes | Yes | Yes | No |
| show mac-address-table <cr> | Yes | Yes | Yes | No |
| show parser-dump | Yes | Yes | Yes | No |
| show privileges <cr> | Yes | Yes | Yes | No |
| show privileges server <cr> | Yes | Yes | Yes | No |
| show report availability <cr> | Yes | Yes | Yes | No |
| show report cpu-utilization <cr> | Yes | Yes | Yes | No |
| show report device-list <cr> | Yes | Yes | Yes | No |
| show report if-performance-summary <cr> | Yes | Yes | Yes | No |
| show report if-utilization-summary <cr> | Yes | Yes | Yes | No |
| show report software <cr> | Yes | Yes | Yes | No |
| show running-config <cr> | Yes | Yes | No | No |
| show running-config archive ARCHIVE-FILE <cr> | Yes | Yes | No | No |
| show running-config device A.B.C.D ARCHIVE-FILE <cr> | Yes | Yes | No | No |
| show running-config diff-with archive ARCHIVE-FILE <cr> | Yes | Yes | No | No |
| show running-config diff-with label LABEL <cr> | Yes | Yes | No | No |
| show running-config diff-with startup-config <cr> | Yes | Yes | No | No |
| show running-config list-archives <cr> | Yes | Yes | No | No |
| show running-config list-archives device A.B.C.D <cr> | Yes | Yes | No | No |
| show server device-packages <cr> | Yes | No | No | No |
| show server event-queues <cr> | Yes | No | No | No |
| show server ip-aliases <cr> | Yes | No | No | No |
| show server known-devices <cr> | Yes | No | No | No |
| show server log <cr> | Yes | No | No | No |
| show server log bookmark WORD <cr> | Yes | No | No | No |
| show server log LOG-FILE <cr> | Yes | No | No | No |
| show server modules <cr> | Yes | No | No | No |
| show server netstat tcp <cr> | Yes | No | No | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| show server netstat udp <cr> | Yes | No | No | No |
| show server routes <cr> | Yes | No | No | No |
| show server running-config <cr> | Yes | No | No | No |
| show server running-config module MODULE <cr> | Yes | No | No | No |
| show server startup-config <cr> | Yes | No | No | No |
| show server stats <cr> | Yes | No | No | No |
| show server thread-pools <cr> | Yes | No | No | No |
| show server threads <cr> | Yes | No | No | No |
| show server translate-packages [ details <from dev-os> <to dev-os> ] <cr> | Yes | Yes | Yes | No |
| show server version <cr> | Yes | No | No | Yes |
| show server version brief <cr> | Yes | No | No | Yes |
| show spanning-tree <cr> | Yes | Yes | Yes | No |
| show spanning-tree vlan <VLAN-ID> <cr> | Yes | Yes | Yes | No |
| show spanning-tree vlan <VLAN-ID> port-state <cr> | Yes | Yes | Yes | No |
| show startup-config <cr> | Yes | Yes | No | No |
| show startup-config archive ARCHIVE-FILE <cr> | Yes | Yes | No | No |
| show startup-config device A.B.C.D ARCHIVE-FILE <cr> | Yes | Yes | No | No |
| show startup-config diff-with archive ARCHIVE-FILE <cr> | Yes | Yes | No | No |
| show startup-config diff-with label LABEL <cr> | Yes | Yes | No | No |
| show startup-config diff-with running-config <cr> | Yes | Yes | No | No |
| show startup-config label LABEL <cr> | Yes | Yes | No | No |
| show startup-config list-archives <cr> | Yes | Yes | No | No |
| show startup-config list-archives device A.B.C.D <cr> | Yes | Yes | No | No |
| show status connections <cr> | Yes | Yes | Yes | No |
| show status connections all <cr> | Yes | Yes | Yes | No |
| show status inventory <cr> | Yes | Yes | Yes | No |
| show terminal <cr> | Yes | Yes | Yes | No |
| show terminal env <cr> | Yes | Yes | Yes | No |
| show version <cr> | Yes | Yes | Yes | Yes |
| show version brief <cr> | Yes | Yes | Yes | Yes |
| show vlan <cr> | Yes | Yes | Yes | No |
| show vlan counters <cr> | Yes | Yes | Yes | No |
| show vlan ports <cr> | Yes | Yes | Yes | No |
| show vtp status <cr> | Yes | Yes | Yes | No |
| show vlan trunk-ports <cr> | Yes | Yes | Yes | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| start debug-log <cr> | Yes | Yes | No | No |
| stop debug-log <cr> | Yes | Yes | No | No |
| subscribe syslog <cr> * | Yes | No | No | No |
| sync archives-with-db <cr> | Yes | No/Yes | No | No |
| sync archives-with-db all <cr> | Yes | No/Yes | No | No |
| sync arp-table <cr> | Yes | Yes | No | No |
| sync asset fg <cr> | Yes | Yes | Yes | No |
| sync asset bg <cr> | Yes | Yes | Yes | No |
| sync config <cr> | Yes | Yes | Yes | No |
| sync config fg <cr> * | Yes | Yes | Yes | No |
| sync config bg <cr> * | Yes | Yes | Yes | No |
| sync filesystem fg <cr> * | Yes | Yes | Yes | No |
| sync filesystem bg <cr> * | Yes | Yes | Yes | No |
| sync stp <cr> | Yes | Yes | No | No |
| sync vtp <cr> | Yes | Yes | No | No |
| system prompt <prompt expression> <cr> | Yes | No | No | No |
| tar create <OUTPUTFILE><InputFileOrDirectory> [InputFileOrDirectory …] <cr> | Yes | Yes | No | No |
| tar extract <INPUTFILE> <OUTPUTDIR> <cr> | Yes | Yes | No | No |
| tar list <INPUTFILE> <cr> | Yes | Yes | No | No |
| terminal color <cr> | Yes | Yes | Yes | Yes |
| terminal cursor-wrap <cr> | Yes | Yes | Yes | Yes |
| **terminal device-auth login <login val> <cr>** | Yes | Yes | Yes | Yes |
| terminal device-id dns-name <cr> | Yes | Yes | Yes | Yes |
| terminal device-id dns-name-short <cr> | Yes | Yes | Yes | Yes |
| terminal device-id ip <cr> | Yes | Yes | Yes | Yes |
| terminal device-id name <cr> | Yes | Yes | Yes | Yes |
| terminal format-report <cr> | Yes | Yes | Yes | Yes |
| terminal ftp-auth username <name> | Yes | Yes | Yes | Yes |
| terminal http-auth <no> | Yes | Yes | Yes | Yes |
| terminal http-auth username <no> | Yes | Yes | Yes | Yes |
| terminal http-auth username WORD <cr> <no> | Yes | Yes | Yes | Yes |
| terminal interactive <cr> | Yes | Yes | Yes | Yes |
| terminal length <0-1> <cr> | Yes | Yes | Yes | Yes |
| terminal length <2-256> <cr> | Yes | Yes | Yes | Yes |
| terminal monitor <cr> | Yes | Yes | Yes | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| terminal monitor message-filter WORD <cr> | Yes | Yes | Yes | No |
| terminal no color <cr> | Yes | Yes | Yes | Yes |
| terminal no device-auth <cr> | Yes | Yes | Yes | Yes |
| terminal no http-auth <cr> | Yes | Yes | Yes | Yes |
| terminal no interactive <cr> | Yes | Yes | Yes | Yes |
| terminal no monitor <cr> | Yes | Yes | Yes | No |
| terminal no monitor message-filter <cr> | Yes | Yes | Yes | No |
| terminal no skip-locked <cr> | Yes | Yes | Yes | Yes |
| terminal no skip-unauth <cr> | Yes | Yes | Yes | Yes |
| terminal no status-codes <cr> | Yes | Yes | Yes | Yes |
| terminal no supress-repeats <cr> | Yes | Yes | Yes | Yes |
| terminal prompt <prompt expression> <cr> | Yes | Yes | Yes | Yes |
| terminal save properties <cr> | Yes | Yes | Yes | Yes |
| terminal set WORD <cr> | Yes | Yes | Yes | Yes |
| terminal set WORD WORD <cr> | Yes | Yes | Yes | Yes |
| terminal skip-locked <cr> | Yes | Yes | Yes | Yes |
| terminal skip-unauth <cr> | Yes | Yes | Yes | Yes |
| terminal status-codes <cr> | Yes | Yes | Yes | Yes |
| terminal stream-ctl read-file FILENAME <cr> | Yes | Yes | Yes | Yes |
| terminal stream-ctl write-file FILENAME <cr> | Yes | Yes | Yes | Yes |
| terminal stream-ctl xml-data-channel <cr> | Yes | Yes | Yes | Yes |
| terminal stream-ctl xml-data-channel WORD <cr> | Yes | Yes | Yes | Yes |
| terminal supress-repeats <cr> | Yes | Yes | Yes | Yes |
| terminal unset WORD <cr> | Yes | Yes | Yes | Yes |
| terminal width <16-256> <cr> | Yes | Yes | Yes | Yes |
| transform x2c FILENAME | Yes | Yes | No | No |
| transform x2c FILENAME server | Yes | Yes | No | No |
| transform c2x FILENAME server | Yes | Yes | No | No |
| transform c2x FILENAME DEVICEFAMILY OSVERSION WORD | Yes | Yes | No | No |
| transform c2x FILENAME DEVICEFAMILY OSVERSION WORD WORD | Yes | Yes | No | No |
| translate file filename <from dev-os> <to dev-os> <cr> | Yes | Yes | Yes | No |
| translate device running <ip address> <to dev-os> <cr> | Yes | Yes | Yes | No |
| translate device startup <ip address> <to dev-os> <cr> | Yes | Yes | Yes | No |
| validate xml-config FILENAME <cr> | Yes | Yes | Yes | Yes |
| verify syntax device Device family FILENAME <cr> | Yes | Yes | No | No |

*Table B-1 Cisco E-DI Commands and Associated Privileges (continued)*

| Command | Admin | Network Operator | Read-Only User | No Access User |
|---|---|---|---|---|
| verify syntax least-common FILENAME <cr> | Yes | Yes | No | No |
| verify syntax server FILENAME <cr> | Yes | Yes | No | No |
| write <cr> | Yes | No/Yes | No | No |
| write memory <cr> * | Yes | No/Yes | No | No |
| x2c FILENAME server | Yes | Yes | No | No |
| x2c FILENAME WORD WORD | Yes | Yes | No | No |

APPENDIX C

# Open Source License Acknowledgement

Cisco E-DI 2.2 uses third-party open source software subject to the following licenses:

- telnetd
- Java Service Wrapper
- Apache License Version 2.0
- Apache 1.1
- PostgreSQL License
- Javolution 4.1

## telnetd

Java TelnetD library (embeddable telnet daemon)

Copyright (c) 2000-2005 Dieter Wimberger.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the author 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 BY THE COPYRIGHT HOLDER AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Java Service Wrapper

Copyright (c) 1999, 2005 Tanuki Software Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Java Service Wrapper and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of the Software have been derived from source code developed by Silver Egg Technology under the following license:

Copyright (c) 2001 Silver Egg Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

# Apache License Version 2.0

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/ TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License. "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. "Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution." "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless

required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages. 9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives. Copyright [yyyy] [name of copyright owner] Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

# Apache 1.1

```
/ ====================================================================
The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the
following acknowledgment:
"This product includes software developed by the Apache Software Foundation
(http://www.apache.org/)."
Alternately, this acknowledgment may appear in the software itself, if and wherever such
third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or
promote products derived from this software without prior written permission. For written
permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear
in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING,
BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
====================================================================
```

```
This software consists of voluntary contributions made by many individuals on behalf of
the Apache Software Foundation.  For more information on the Apache Software Foundation,
please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the
National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.
 /
```

# PostgreSQL License

License

PostgreSQL is released under the BSD license.

PostgreSQL Database Management System

(formerly known as Postgres, then as Postgres95)



Why not the GNU General Public License?

People often ask why PostgreSQL is not released under the GNU General Public
License. The simple answer is because we like the BSD license and do not want to
change it. If you are keen to read more about this topic, then please take a
look in the Archives at any of the many threads on this subject, but please
don't start yet another debate on the subject!

# Javolution 4.1

```
Javolution - Java(TM) Solution for Real-Time and Embedded Systems
Copyright (c) 2006, Javolution (http://javolution.org)
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

# INDEX

## Symbols



## A



## C

## D

## E

## F



## G



## H



## I



## J



## K

## L



## M

## N



## P



## Q



## R

## S

## T



## U

## V



## W



## Y