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. To you log in, you can use the default username **admin**, and password **admin**. After you log in, you can create a new username and change your password if required.
- 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.

# 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*

| Description | 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**] **aaa 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** <*ipaddress*>.

# 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 nonsession-based device authentication mode. Nonsession-based device authentication is selected by default. A user can switch between session-based and nonsession-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 nonsession-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.

## NonSession-Based Device Authentication

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

If the administrator selects nonsession-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 (nonsession-based) device credential stores. The administrator is required to preconfigure 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 preconfigured 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, the nonsession-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. Refer to *Release Notes for Cisco Enhanced Device Interface 2.2.1.*

# 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.

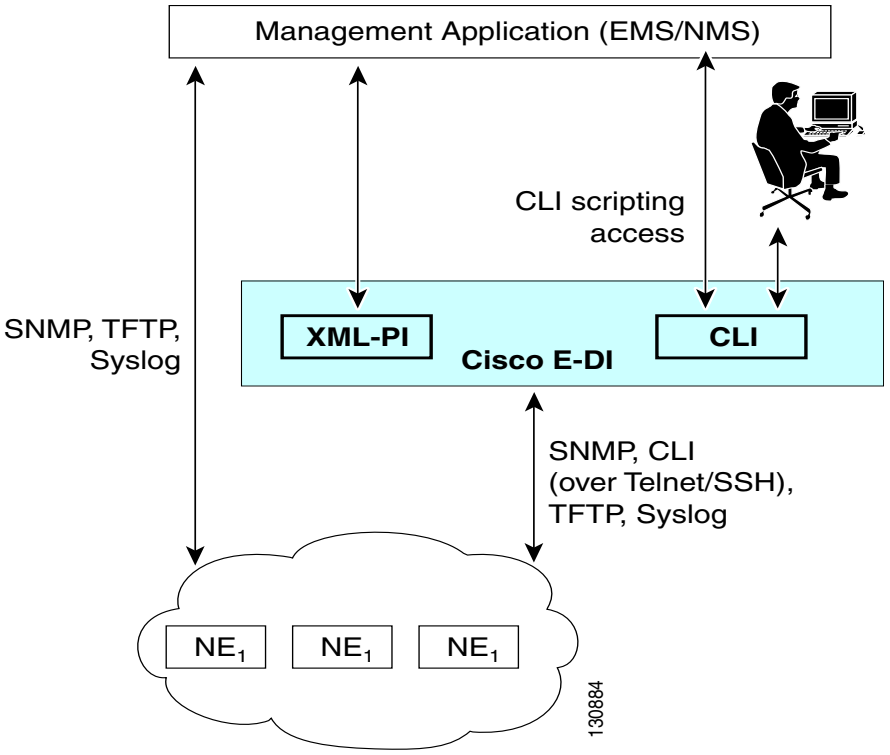
There are three related concepts in Cisco E-DI:

- 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 submodes 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 predefined submodes which in turn have multiple submodes:

- 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 2-7 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:

- 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.

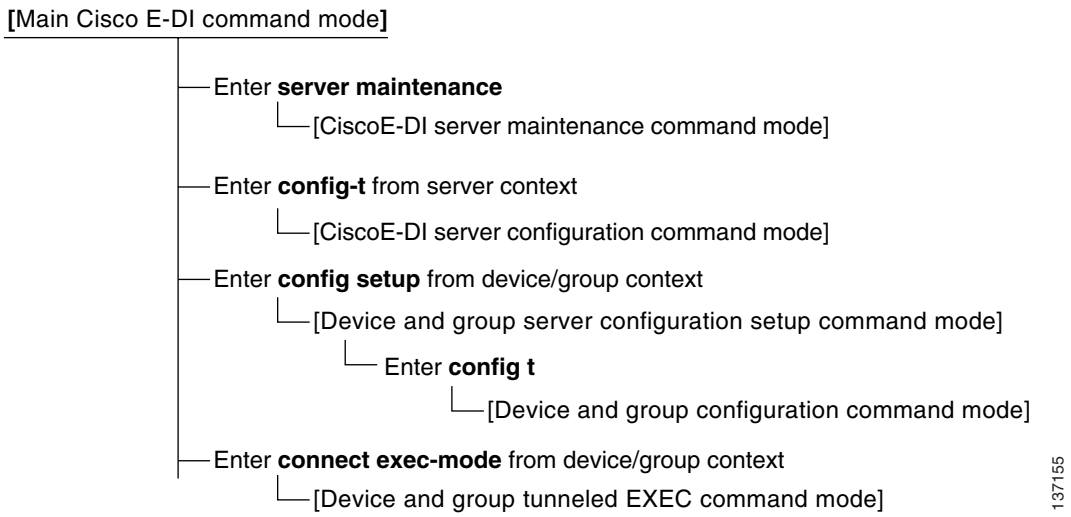
- Device and group tunneled EXEC command mode

  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 1-3 shows the hierarchy and relationship of the 6 basic CLI modes.

***Figure 1-3 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 3-11. 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] #` |

*Table 1-3 Configuration Submodes (continued)*

| Command | Command Mode |
|---|---|
| `[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 2.2.1 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).

# 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 2-7 for a full explanantion 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 |
| 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 |

*Table 1-4 Device Capabilities (continued)*

| Name | Device capability |
|---|---|
| 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 |
| 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 |

*Table 1-5 Interface Groups (continued)*

| Name | Description |
|---|---|
| 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**.