ROLE-BASED COMMAND-LINE INTERFACE ACCESS

DENISE HELFRICH

MARCH 2004

Agenda

- Role-Based Command-Line Interface (CLI) Access Overview
- Configuration Tasks
  - CLI Views
  - Lawful Intercept View
- How to access and use a view
- Resources
- Summary

ROLE-BASED CLI ACCESS

Role-Based User Views

Administrator

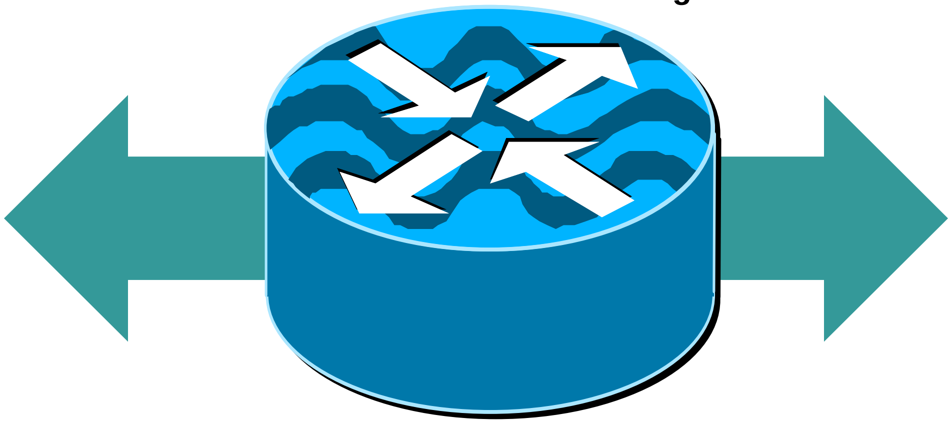
LAN Engineer

DBMS/Application Engineer

Service Desk

Capacity Planner

- Show
- Etc



Customized Access To Match Operational Needs

WAN Engineer

- Config
- Show
- Etc

Role-Based CLI Access Benefits

- **Security**

  Enhances the security of a device by defining the set of CLI commands accessible to a user

- **Availability**

  Avoids unintentional executions of CLI commands by unauthorized personnel

- **Operational Efficiency**

  Greatly improves usability by prohibiting users from viewing CLI commands that are inaccessible to them

Role-Based CLI Access Functions

- Available in Cisco IOS® Software Release 12.3(7)T
- Up to sixteen CLI Views
  - Role-based views
  - One “root” view
  - Up to fifteen custom views
  - Standard feature in all Cisco IOS Software images
- Lawful Intercept view
  - Confidential electronic surveillance view
  - One Lawful Intercept view
  - Available in 3DES K9 images
  - Export restrictions apply

How it Works

- An administrator must define views using the “root” view
  - No default views
  - Must have privilege level fifteen to access the root view
  - Must create a view and specify the allowed commands
- A user can access a view
  - Manually enter a view name and password
  - View is automatically assigned via username login
  - When users are in a view, they can only use commands specified for that view
  - Users can switch between views if they know the view name and password

CLI VIEWS CONFIGURATION

How CLI View Relates to Other Configurations

- **Authentication Authorization and Accounting (AAA)**

  AAA must first be enabled with the `aaa new-model` command

  One view name is associated with a user in the local database or external AAA server

  At login, a user is placed in a view after the usual user authentication

- **Privilege Level**

  View name takes precedence over the privilege level

  User is placed in the privilege level if the view does not exist

- **View Name**

  Only one view name can be configured for a user

  If the view name is not configured, the user is set to existing privilege level

  View names and passwords are case sensitive

CLI View Configuration Tasks

- **Prerequisite Configuration**
- **Task 1: login to Root view**
- **Task 2: configure a new view**
- **Task 3: access a CLI view**
- **Task 4: assign username view level**

Prerequisite Configuration

- The “enable” password must exist
  - Password encryption is recommended
  - For better security, use “enable secret” password
  - To access root view the passwords are:
    - Enable secret (if present)
    - Enable password (if enable secret is not present)
- AAA must first be enabled with the `aaa new-model` command
- Root view user must have privilege fifteen level assigned via the privilege command

Task 1: Login to Root View

Router#

```
enable view
```

```
Router# enable view
Password:       |enter enable or enable secret password

*Mar  18 00:04:28.891: %PARSER-6-VIEW_SWITCH:
successfully set to view 'root'

Router#
```

Note: “% Authentication failed” message returns if a user unsuccessfully authenticates

Task 2: Configure a New View

Step 1: Create the New View and Enter Config-View Mode

Router(config)#

```
parser view view-name
```

```
Router# configure terminal
Router(config)# parser view Admin123

*Mar  18 01:07:56.167: %PARSER-6-VIEW_CREATED:
view ‘Admin123' successfully created.

Router(config-view)#
```

Notes:

- The no form of parser view view-name is used to delete the view
- View name is case sensitive

Task 2: Configure a New View (Cont.)

Step 2: Create the View Password

Router(config-view)#

```
password 5 view-password
```

```
Router(config-view)# password 5 Admin@Pswd
```

Note: Password is case sensitive

Task 2: Configure a New View (Cont.)

Step 3: Add Commands Allowed to Use for this View

Router(config-view)#

```
commands parser-mode {include | include-exclusive}
  [all] command
```

```
Router(config-view)# commands exec include show
interfaces

Router(config-view)# commands exec include all

Router(config-view)# commands configure include-
exclusive crypto
```

Notes:

- Implicit deny all
- Must include the command
- Include-exclusive command includes command for this view while excluding it in all other views

Task 3: Access a CLI View

Step 1: Manually Access a View

Router#

```
enable view view-name
```

```
Router# enable view Admin123

Password: Admin@Pswd

*Mar  18 02:15:18.035: %PARSER-6-VIEW_SWITCH:
successfully set to view ‘Admin123'

Router#
```

Example: Acme Company Access Roles

Network OPS Administrator

- Some EXEC
- Some Router Config
- No Security Config

Security OPS Administrator

- Show Everything
- EXEC Copy Run only
- EXEC Crypto
- Security Config

Operator

- Ping
- Show Hardware
- Show Interfaces
- Show Version

WAN Engineer

- Everything

Acme Company Operator View Sample Configuration

```
Router# enable view
Password:secretpswd
*Mar  18 02:15:18.035: %PARSER-6-VIEW_SWITCH: successfully
set to view ‘root'
Router# configure Terminal
Router(config)# parser view operator
Router(config-view)#password 5 Oper@torPswd
Router(config-view)#commands exec include ping
Router(config-view)#commands exec include show hardware
Router(config-view)#commands exec include show interfaces
Router(config-view)#commands exec include show version
Router(config-view)#exit
Router(config)#
```

Acme Company Network Administrator View Sample Configuration

```
Router(config)# parser view NetOps
Router(config-view)#password 5 NetOps@Pswd
Router(config-view)#commands exec include clear
Router(config-view)#commands exec include copy
Router(config-view)#commands exec include ping
Router(config-view)#commands exec include all show
Router(config-view)#commands exec include configure
Router(config-view)#commands configure include access-list
Router(config-view)#commands configure include clock
Router(config-view)#commands configure include hostname
Router(config-view)#commands configure include interface
Router(config-view)#commands configure include ip
Router(config-view)#commands configure include line
Router(config-view)#exit
Router(config)#
```

Acme Company Security Administrator View Sample Configuration

```
Router(config)# parser view SecOps
Router(config-view)#password 5 SecOps@Pswd
Router(config-view)#commands exec include copy running-config
Router(config-view)#commands exec include login
Router(config-view)#commands exec include all show
Router(config-view)#commands exec include-exclusive show crypto
Router(config-view)#commands exec include-exclusive show key
Router(config-view)#commands exec include configure terminal
Router(config-view)#commands configure include access-list
Router(config-view)#commands configure include-exclusive crypto
Router(config-view)#commands configure include-exclusive key
Router(config-view)#commands configure include-exclusive li-view
Router(config-view)#exit
Router(config)#
```

Acme Company Security Engineer Sample Configuration

```
Router(config)#username engineer privilege 15 password enGr=9l1
```

- Access to all EXEC and configuration commands
- Easiest method is to assign them a privilege fifteen level

View Capabilities

Operator

```
Router#enable view operator
Password: Oper@torPswd
*…view 'operator'
Router# ?
Exec commands:
 exit
 ping
 show
Router#show ?
 hardware
 interfaces
 version
```

NetOps

```
Router#enable view NetOps
Password: NetOps@Pswd
*…view ‘NetOps'
Router# ?
Exec commands:
 clear
 configure
 copy
 enable
 exit
 ping
 show
Router#show ?
 controllers
 hardware
 interfaces
 version
Router#configure terminal
Router(config)#?
 access-list
 clock
 hostname
 interface
 ip
 line
```

SecOps

```
Router#enable view SecOps
Password: SecOps@Pswd
*…view ‘SecOps'
Router# ?
Exec commands:
 configure
 copy
 enable
 exit
 login
 ping
 show
Router#show ?
 controllers
 crypto
 hardware
 interfaces
 key
 version
Router#configure terminal
Router(config)#?
 access-list
 crypto
 key
 li-view
```

Task 4: Assign Username View Level

Router(config)#

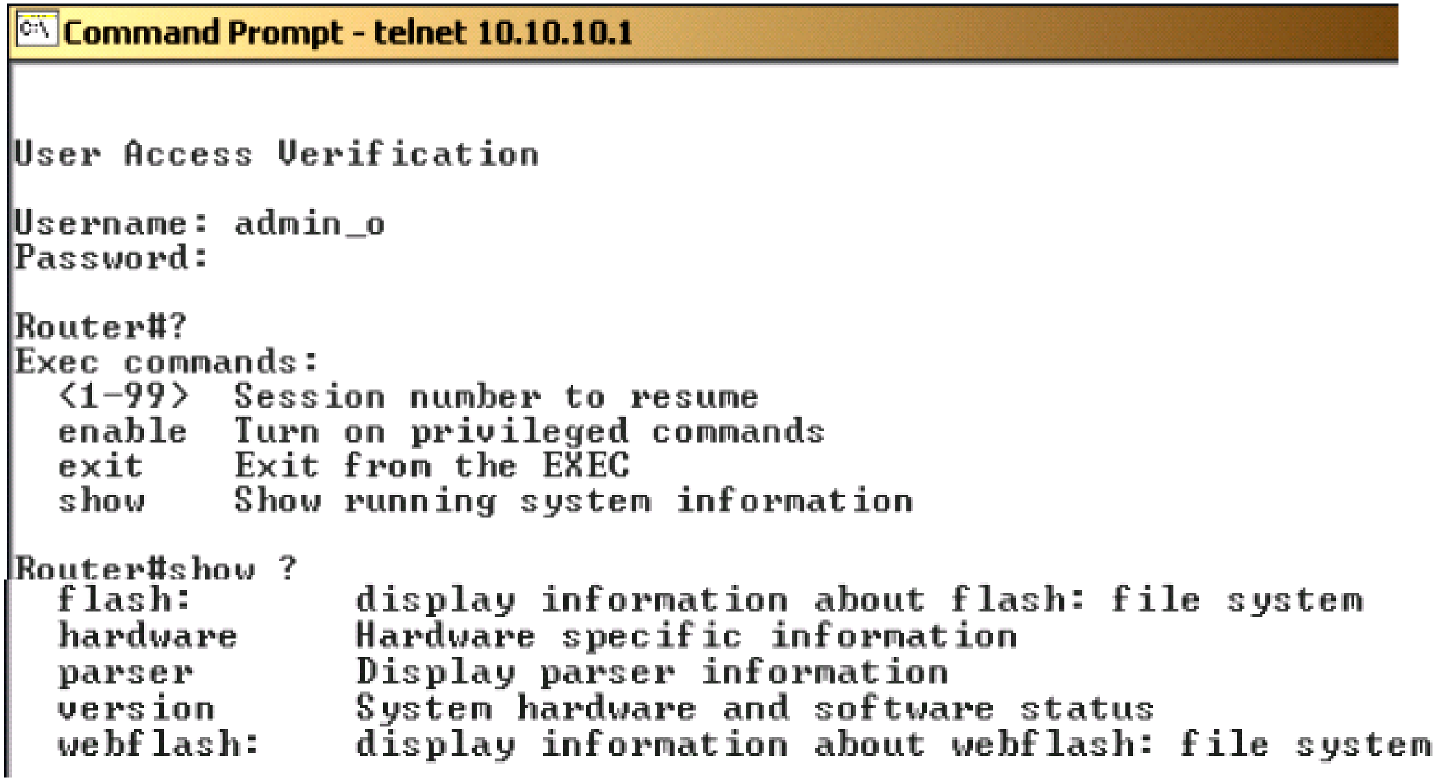
```
username name {privilege privilege-level | view
  view-name] password password}
```

```
Router(config)# username admin_o view operator
password chF&9l$

Router(config)# username admin_n view NetOps
password kz7pE%t

Router(config)# username admin_s view SecOps
password p8eWo*i
```

- User automatically enters an assigned view upon successful login
- User can manually switch views with enable view *view-name view-password*

Example: Login and Views for Admin_o User

Cisco.com



Command Prompt - telnet 10.10.10.1

```


User Access Verification

Username: admin_o
Password:

Router#?
Exec commands:
  <1-99>  Session number to resume
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  show    Show running system information

Router#show ?
  flash:        display information about flash: file system
  hardware      Hardware specific information
  parser        Display parser information
  version       System hardware and software status
  webflash:     display information about webflash: file system
```

LAWFUL INTERCEPT VIEW CONFIGURATION

Lawful Intercept View

- Service Providers should be able to implement authorized and undetectable electronic surveillance
- Lawful Intercept is available in special 3DES Crypto K9 images found in hardware that supports Cisco IOS Software Release 12.3(7)T
- Able to monitor packets flowing through a Cisco router
- Copies packets and sends them to the Mediation Device for further processing
- Lawful Intercept user can only access lawful intercept commands that are held within the TAP-Management Information Base (MIB)

  Special set of Simple Network Management Protocol (SNMP) commands

  Stores information about calls and users
- One Lawful Intercept view

Lawful Intercept Configuration Tasks

- **Task 1: login to Root view**
- **Task 2: configure a Lawful Intercept view**
- **Task 3: access Lawful Intercept view**

Task 1: Login to Root View

Router#

```
enable view
```

```
Router# enable view
Password:       |enter enable or enable secret password

*Mar  18 00:04:28.891: %PARSER-6-VIEW_SWITCH:
successfully set to view 'root'

Router#
```

Note: “% Authentication failed” message returns if a user unsuccessfully authenticates

Task 2: Configure a Lawful Intercept View

Step 1: Initialize Lawful Intercept View

Router(config)#

li-view *li-password* user *username* password *password*

```
Router# configure terminal
Router(config)# li-view 5eg4w0pi user li_admin
password n*s3Np7

*Mar 18 13:37:06.907: %PARSER-6-LI_VIEW_INIT: LI-View
initialised.

Router(config)#exit
```

Notes:

- **Only level fifteen privilege user can initialize a Lawful Intercept view**
- **At least one user must be specified**

Task 2: Configure a Lawful Intercept View (Cont.)

Step 2: (Optional) Create Users with the Lawful Intercept Option Upon Login

Router(config)#

```
username [lawful-intercept name][privilege privilege-
  level | view view-name] password password]
```

```
Router# configure terminal
Router(config)# username lawful-intercept LI-user1
password c9Sq&v1

*Mar 18 13:37:06.907: %PARSER-6-LI_VIEW_INIT: LI-View
initialised.

Router(config)#
```

Task 2: Configure a Lawful Intercept View (Cont.)

Step 3: (Optional) Edit Lawful Intercept View

Router(config)#

```
Router(config)#parser view view-name

Router(config-view)# password 5 password

Router(config-view)# name new-name

Router(config-view)# commands parser-mode {include |
  include-exclusive} [all] command

Router(config-view)# exit
```

Note: Lawful Intercept view defaults with all allowed commands

Task 3: Access Lawful Intercept View

Router#

```
Router# enable view li-view
Password:                |enter li-password
*Mar 18 15:38:36.151: %PARSER-6-VIEW_SWITCH:
  successfully set to view 'li-view'
Router#
```

Monitoring Views and View Users

- Displays information about the view that the user is currently in

```
Router# show parser view [all]
```

```
Router# show parser view
Current view is 'li-view'
Router#
```

- Displays all users, who have access to a Lawful Intercept view

```
Router# show users [lawful-intercept]
```

```
Router# show users lawful-intercept
li_admin
LI-user1
Router#
```

Resources

- **Cisco IOS Software Release 12.3(7)T**

  www.cisco.com/go/release123t

- **Lawful Intercept Design Guides**

  www.cisco.com/en/US/partner/tech/tk583/tk799/tech_design_guides_list.html

- **Cisco IOS Infrastructure Security**

  www.cisco.com/go/autosecure/

- **Cisco IOS Software Collateral Library**

  www.cisco.com/go/library/