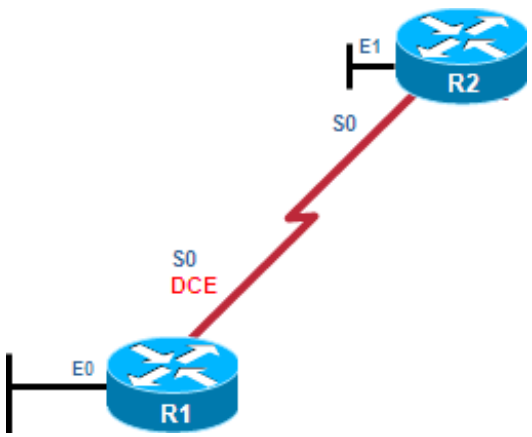
CIS 4080
Network Security

Securing Network Devices, Part 2

Configuring SSH



- Step 1: Configure the IP domain name.
- Step 2: Generate RSA keys.
- Step 3: Create a local database username entry.
- Step 4: Enable VTY inbound SSH sessions.

```
R1# configure terminal
R1(config)# ip domain-name cislab.vtc.edu
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

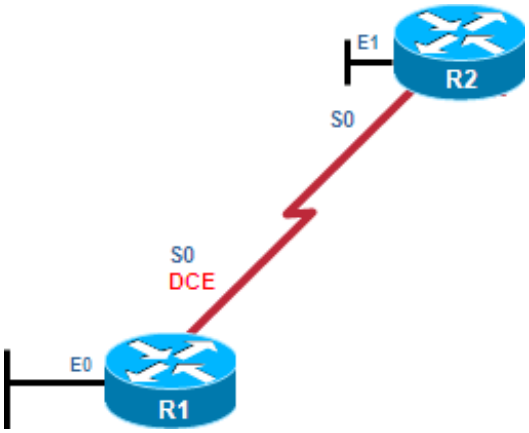
Optional SSH Features

- Optionally, SSH commands can be used to configure the following:
  - SSH version
  - Number of authentication retries
  - SSH timeout period

Optional SSH Features

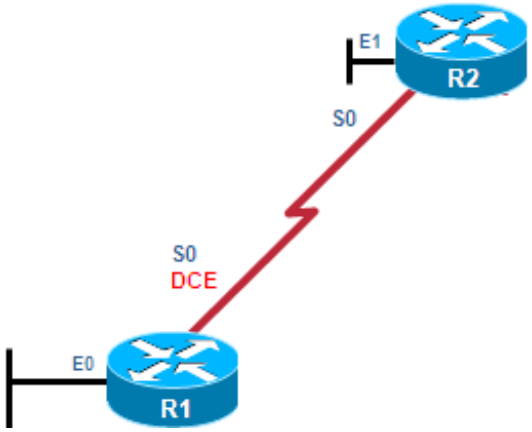
- **SSH Versions:**
  - Cisco IOS Release 12.1(1)T and later supports SSHv1.
  - Cisco IOS Release 12.3(4)T and later supports both SSHv1 and SSHv2 (compatibility mode).
  - To change versions, use the **`ip ssh version {1 | 2}`** global command. *NOTE: Version 1 is obsolete. Do not use it!*
- **Number of authentication retries:**
  - By default, a user logging in has 3 attempts before being disconnected.
  - To configure a different number of consecutive SSH retries, use the **`ip ssh authentication-retries`** *`integer`* command in global configuration mode.
- **SSH Timeouts:**
  - The default time interval that the router will wait for an SSH client to respond during SSH negotiation phase is 120 seconds.
  - Change the time using **`ip ssh time-out`** *`seconds`*.

Optional SSH Commands




```
R1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh version 2
R1(config)# ip ssh authentication-retries 2
R1(config)# ip ssh time-out 60
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 2
R1#
```

Router-to-Router SSH



2 R2 establishes an SSH connection with R1.

```
R2# ssh -l Bob 192.168.2.101

Password:

R1>
```

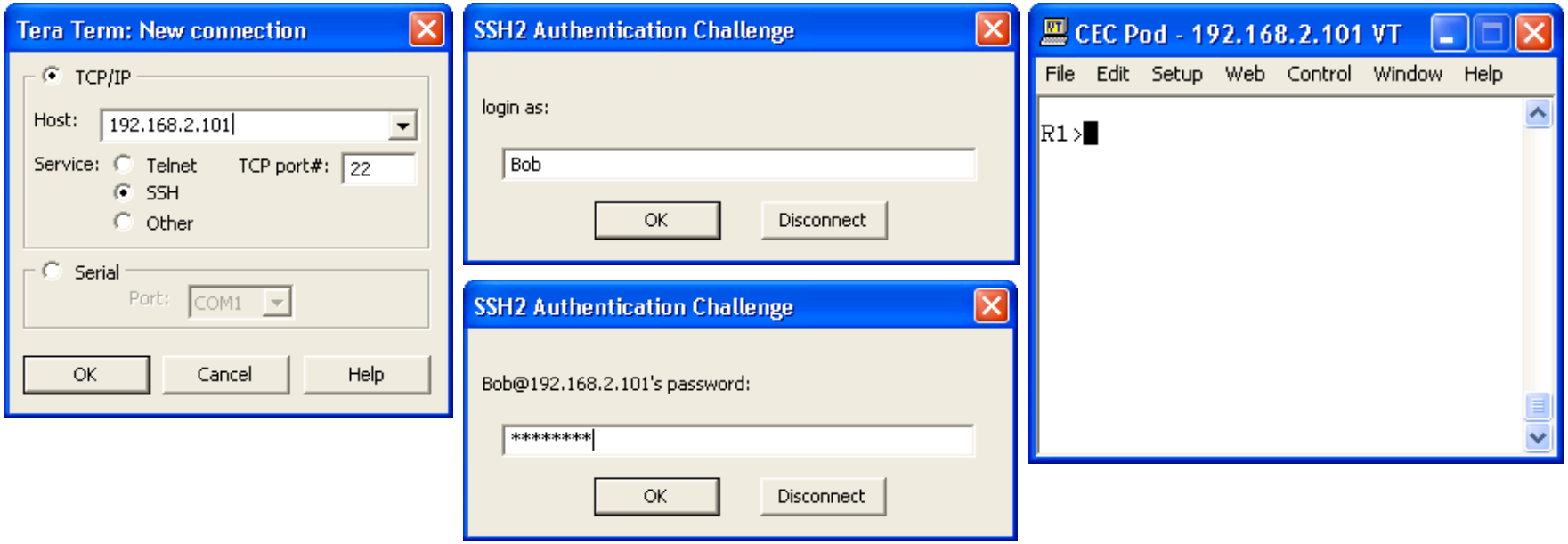
1 There are no current SSH sessions ongoing with R1.

```
R1# show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R1#
```

3 There is an incoming and outgoing SSHv2 session with user Bob.

```
R1# show ssh
Connection   Version Mode Encryption   Hmac         State              Username
0            2.0     IN   aes128-cbc   hmac-sha1  Session started      Bob
0            2.0     OUT  aes128-cbc   hmac-sha1  Session started      Bob
%No SSHv1 server connections running.
R1#
```

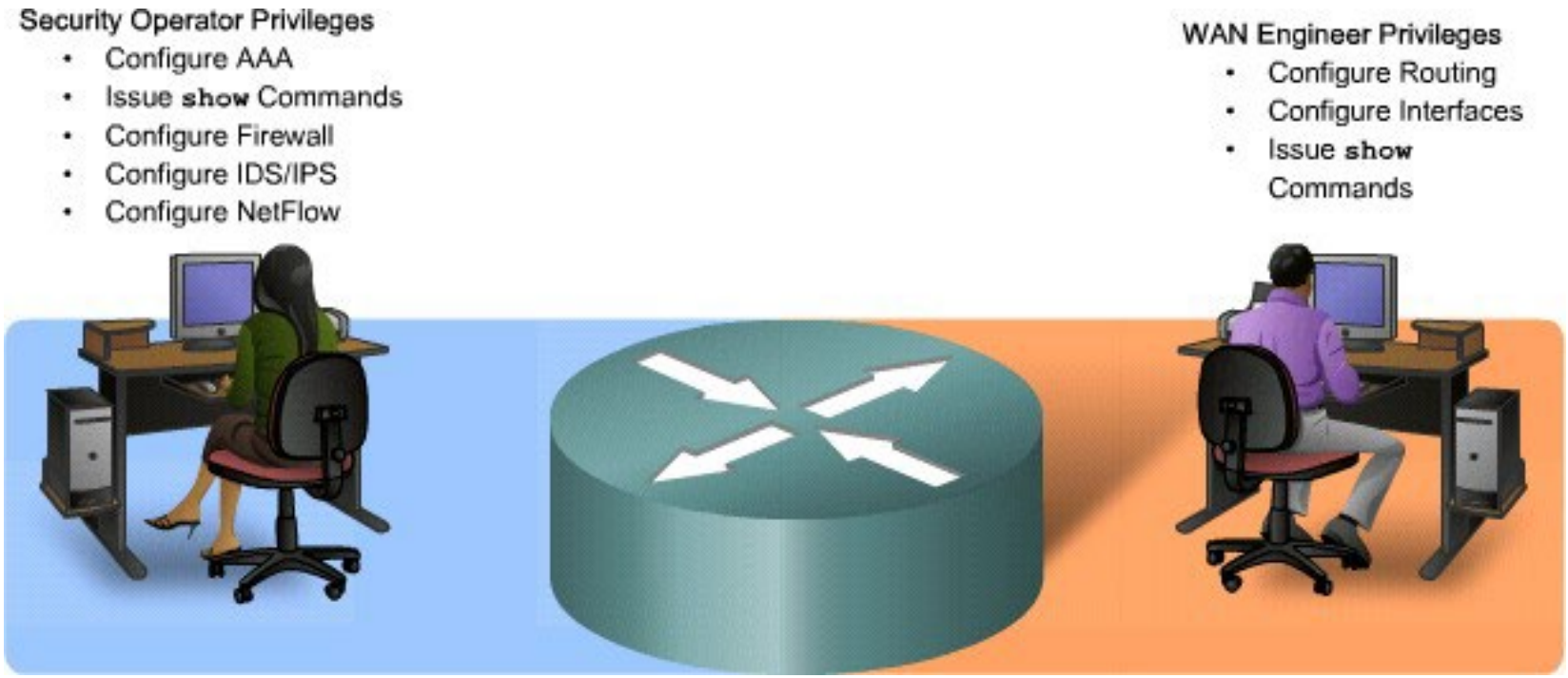
Host-to-Router SSH



Question!

- Should everyone in an IT department have the same level of access to the network infrastructure (routers, switches, AP, …)?
- No!
- Configure either:
  - Privilege levels
  - Role-Based CLI

Privilege Levels



Privilege Levels

- The needs of a network security operator may not be the same as that of WAN engineer.
- Cisco routers allow configuration at various privilege levels for administrators.
  - Different passwords can be configured to control who has access to the various privilege levels.
- There are 16 privilege levels.
  - Levels 2 to 14 can be configured using the **`privilege`** global configuration command.

Privilege Levels

- Level 0:
  - Predefined for user-level access privileges.
  - Seldom used, but includes five commands: **`disable`**, **`enable`**, **`exit`**, **`help`**, and **`logout`**.
- Level 1(User EXEC mode):
  - The default level for login with the router prompt **`Router>`**.
  - A user cannot make any changes or view the running configuration file.
- Levels 2 –14:
  - May be customized for user-level privileges.
  - Commands from lower levels may be moved up to a higher level, or commands from higher levels may be moved down to a lower level.
- Level 15 (Privileged EXEC mode):
  - Reserved for the enable mode privileges (**`enable`** command).
  - Users can view and change all aspects of the configuration.

Router Privilege Levels

```
Router(config)#
privilege mode {level level command | reset command}
```

Command	Description
mode	This command argument specifies the configuration mode. Use the privilege ? command to see a list of router modes.
level	(Optional) This command enables setting a privilege level with a specified command.
level command	(Optional) This parameter is the privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) This command resets the privilege level of a command.
command	(Optional) This is the command argument to use when you want to reset the privilege level.

Router Privilege Levels Example

- In this example, four user accounts were created.
  - A USER account with normal Level 1 access.
  - A SUPPORT account with Level 1 and **`ping`** command access.
  - A JR-ADMIN account with the same privileges as the SUPPORT account plus access to the **`reload`** command.
  - An ADMIN account which as all the regular privileged EXEC commands.

```
R1# configure terminal
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
R1(config)#
```

Router Privilege Levels

- The administrator tests the accounts and logs in as the Level 1 user.
  - Usernames are not case-sensitive by default.
  - The **`ping`** command which is typically available from Level 1 is no longer available.

```
User Access Verification

Username: user
Password: <cisco>
R1> show privilege
Current privilege level is 1
R1# ping 10.10.10.1
     ^
% Invalid input detected at '^' marker.

R1>
```

Router Privilege Levels

- The administrator now verifies the Level 5 access.
  - The **`enable`** *`level`* command is used to switch from Level 1 to Level 5.

```
R1> enable 5
Password:<cisco5>
R1#
R1# show privilege
Current privilege level is 5
R1#
R1# ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
R1# reload
Translating "reload"

Translating "reload"

% Unknown command or computer name, or unable to find computer address
R1#
```

Router Privilege Levels

- The administrator now verifies the Level 10 access.
  - Again, the **`enable`** *`level`* command is used to switch from Level 5 to Level 10.
  - Notice now the **`ping`** command and **`reload`** command are available however, the show **`running-config`** command is not.

```
R1# enable 10
Password:<cisco10>
R1# show privilege
Current privilege level is 10
R1# ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1# reload

System configuration has been modified. Save? [yes/no]: ^C
R1# show running-config
        ^
% Invalid input detected at '^' marker.
R1#
```

Router Privilege Levels

- Finally, the administrator verifies the privileged EXEC Level 15 access.
  - Again, the **`enable`** *`level`* command is used to switch from Level 10 to Level 15.
  - Now all commands are available.

```
R1# enable 15
Password: <cisco123>
R1# show privilege
Current privilege level is 15
R1# show running-config
Building configuration...

Current configuration : 1145 bytes
!
version 12.4

<output omitted>
```

Privilege Level Limitations

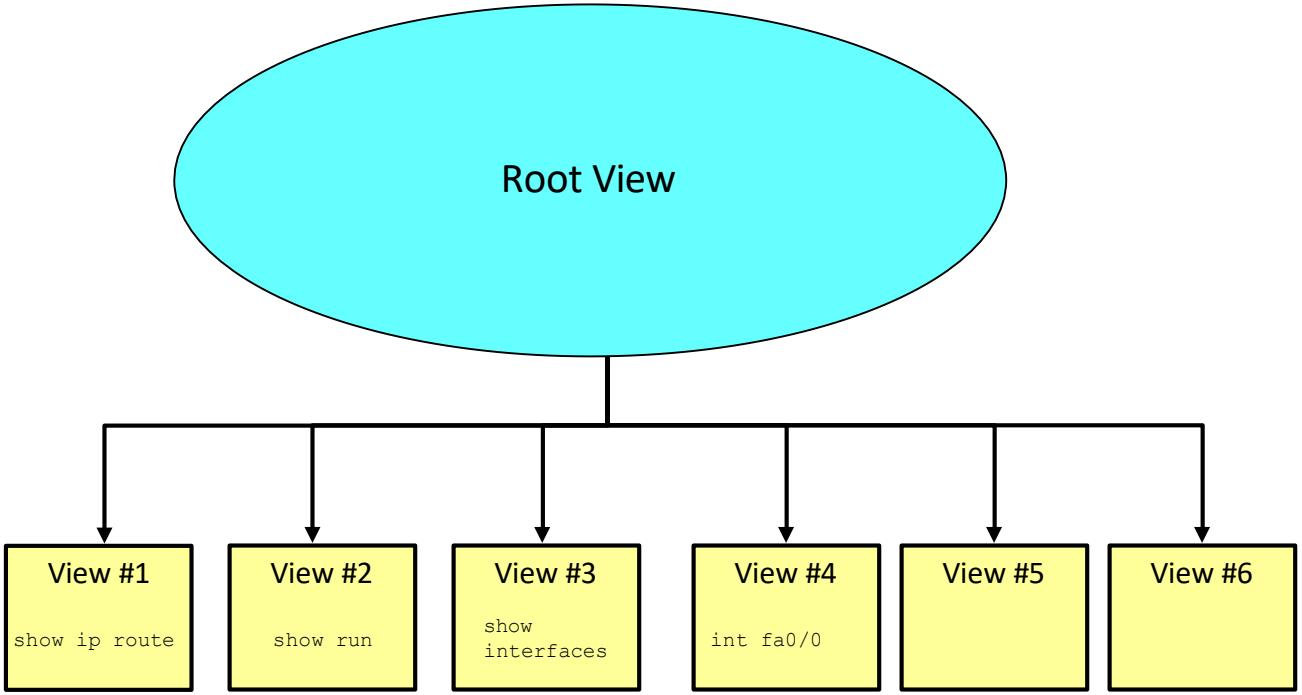
- No access control to specific interfaces, ports, logical interfaces, and slots on a router.
- Commands available at lower privilege levels are always executable at higher levels.
- Commands specifically set on a higher privilege level are not available for lower privileged users.
- Assigning a command with multiple keywords to a specific privilege level also assigns all commands associated with the first keywords to the same privilege level.
  - An example is the **`show ip route`** command.
- If an administrator needs to create a user account that has access to most but not all commands, privilege exec statements must be configured for every command that must be executed at a privilege level lower than 15.
  - This can be a tedious process.

Role-Based CLI Overview

- Privilege levels and enable mode passwords do not provide the necessary level of detail needed when working with Cisco IOS routers and switches.
- The Role-Based CLI Access feature allows the administrator to define “views”.
  - Views are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration mode commands.
  - Views restrict user access to Cisco IOS CLI and configuration information; that is, a view can define what commands are accepted and what configuration information is visible.

Root View

- Root View is required to defines Views and Superviews.
- Views contain commands.
- A command can appear in more than one view.



Role-Based CLI Overview

- Root view is the highest administrative view.
  - Creating and modifying a view or ‘superview’ is possible only from root view.
  - The difference between root view and privilege Level 15 is that only a root view user can create or modify views and superviews.
- Role-Based CLI views require AAA new-model:
  - This is necessary even with local view authentication.
- A maximum of 15 CLI views can exist in addition to the root view.

Getting Started with Role-Based CLI

- Before a view is entered or created, AAA must be enabled via the **`aaa new-model`** command.
- Next, use the **`enable`** command with the **`view`** parameter to enter the root view.
  - e.g., **`enable view`**
  - Optionally you can also use **`enable view root`**.
- Use the privilege 15 password ("`enable secret`"), if prompted for authentication (if authentication is configured).

Getting Started with Role-Based CLI

- Enter a privilege level or a CLI view.
- Use **`enable`** command with the **`view`** parameter to enter the root view.
- Root view requires privilege Level 15 authentication.

```
Router#
enable [privilege-level] [view [view-name]]
```

- The **`aaa new-model`** command must be entered.

```
R1(config)# aaa new-model
R1(config)# exit
R1# enable view
Password:
R1#
%PARSER-6-VIEW_SWITCH: successfully set to view 'root'
```

`enable` Parameters

```
Router#
enable [privilege-level] [view [view-name]]
```

Parameter	Description
privilege-level	(Optional) Sets the privilege level at which to log in.
view	(Optional) If given by itself, enters root view, which enables users to configure CLI views. This keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified CLI view. This keyword can be used to switch from one CLI view to another CLI view.

Configuring CLI Views

- Creates a view and enters view configuration mode.

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

- Sets a password to protect access to the view.

```
Router(config-view)# secret password
Router(config-view)# commands parser-mode {include | include-exclusive | exclude}
[all] [interface interface-name | command]
```

- Example configuration setting a password and adding commands to the view named MONITOR-VIEW.

```
R1(config)# parser view MONITOR-VIEW
R1(config-view)# secret cislab
R1(config-view)# commands exec include show version
```

commands Parameters

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

Parameter	Description
parser-mode	Specifies the mode in which the specified command exists (e.g. exec mode).
include	Adds a command or an interface to the view and allows the same command or interface to be added to an additional view.
include-exclusive	Adds a command or an interface to the view and excludes the same command or interface from being added to all other views.
exclude	Excludes a command or an interface from the view; that is, users cannot access a command or an interface.
all	(Optional) Specifies a "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view.
interface *interface-name*	(Optional) Specifies an interface that is added to the view.
command	(Optional) Specifies a command that is added to the view.

Role-Based CLI Configuration Example

- The CLI view FIRST is created and configured to include the commands **`show version`**, **`configure terminal`**, and all commands starting with **`show ip`**.

```
R1(config)# aaa new-model
R1(config)# exit
R1# enable view
%PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1# configure terminal
R1(config)# parser view FIRST
%PARSER-6-VIEW_CREATED:view 'FIRST' successfully created.
R1(config-view)# secret firstpass
R1(config-view)# command exec include show version
R1(config-view)# command exec include configure terminal
R1(config-view)# command exec include all show ip
R1(config-view)# exit
```

Role-Based CLI Configuration Example

- Next, the administrator will verify the configuration by entering and viewing the available commands.
  - When a user enters the CLI view, an indication message appears.
  - Apart from the commands **`enable`** and **`exit`** that are available in all views, the only two commands that are visible in the CLI view are **`configure`** and **`show`**.

```
R1> enable view FIRST
Password:
%PARSER-6-VIEW_SWITCH:successfully set to view 'FIRST'.
R1# ?
Exec commands:
configure           Enter configuration mode
enable              Turn on privileged commands
exit                Exit from the EXEC
show                Show running system information
```

Role-Based CLI Configuration Example

- To further verify the view configuration, the administrator looks at the available options of the **show** command.
  - The available options include **parser**, which is always available, and the configured keywords **ip** and **version**.

```
R1# show ?
ip                  IP information
parser              Display parser information
version             System hardware and software status
```

Role-Based CLI Configuration Example

- Next, the user verifies that all sub-options of the **`show ip`** command are available in the view.

```
R1# show ip ?
access-lists            List IP access lists
accounting              The active IP accounting database
aliases                 IP alias table
arp                     IP ARP table
as-path-access-list     List AS path access lists
bgp                     BGP information
cache                   IP fast-switching route cache
casa                    Display casa information
cef                     Cisco Express Forwarding
community-list          List community-list
dfp                     DFP information
dhcp                    Show items in the DHCP database drp
--More--
```

Role-Based CLI Configuration Example

- Now assign the view to a user.

```
R1# configure terminal
R1(config)# username Bob view FIRST secret cisco123
```

Another Sample Config

```
R1(config)# parser view SHOWVIEW
*Mar  1 09:54:54.873: %PARSER-6-VIEW_CREATED: view 'SHOWVIEW' successfully
created.
R1(config-view)# secret cisco
R1(config-view)# commands exec include show version
R1(config-view)# exit
R1(config)# parser view VERIFYVIEW
*Mar  1 09:55:24.813: %PARSER-6-VIEW_CREATED: view 'VERIFYVIEW' successfully
created.
R1(config-view)# commands exec include ping
% Password not set for the view VERIFYVIEW
R1(config-view)# secret cisco5
R1(config-view)# commands exec include ping
R1(config-view)# exit
R1(config)# parser view REBOOTVIEW
R1(config-view)#
*Mar  1 09:55:52.297: %PARSER-6-VIEW_CREATED: view 'REBOOTVIEW' successfully
created.
R1(config-view)# secret cisco10
R1(config-view)# commands exec include reload
R1(config-view)# exit
```

Display Views

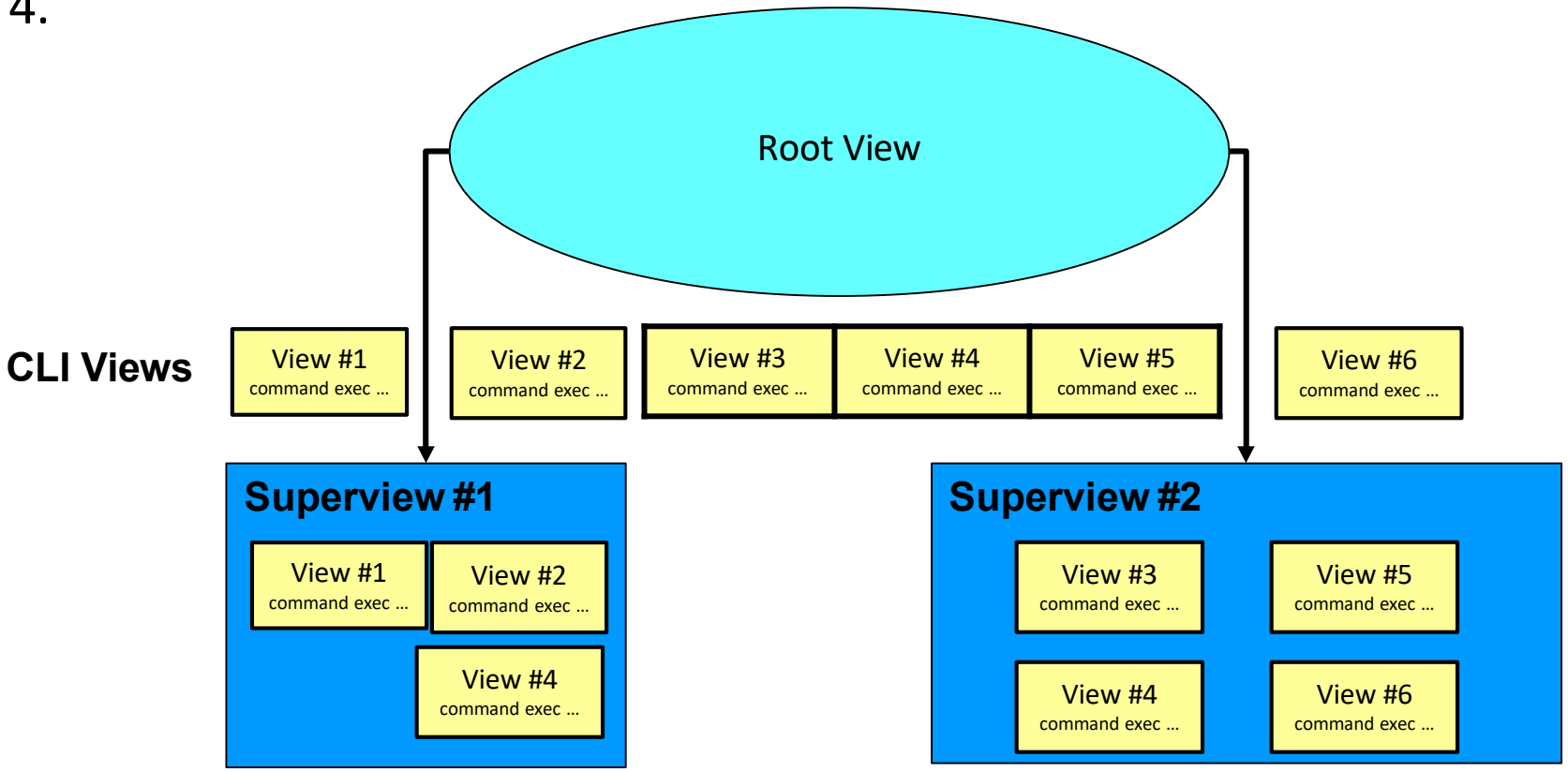
```
R1# show running-config

<Output omitted>

parser view SHOWVIEW
 secret 5 $1$GL2J$8njLecwTaLAc0UuWo1/Fv0
 commands exec include show version
 commands exec include show
!
parser view VERIFYVIEW
 secret 5 $1$d08J$1zOYSI4WainGxkn0Hu7lP1
 commands exec include ping
!
parser view REBOOTVIEW
 secret 5 $1$L7lZ$1Jtn5IhP43fVE7SVoF1pt.
 commands exec include reload
!
```

SuperViews

- Superviews contain Views but not commands.
- Two Superviews can use the same View.
- For example, both Superview 1 and Superview 2 can include CLI View 4.



Superview Characteristics

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview.
  - Commands are added to CLI views.
  - Users who are logged in to a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.
- If a superview is deleted, CLI views associated with that superview are not deleted.

Configure a Superview

- Appending the keyword **superview** to the **parser view** command creates a superview and enters view configuration mode.

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

- Sets a password to protect access to the superview.
- Password must be created immediately after creating a view otherwise an error message will appear.

```
Router(config-view)# secret encrypted-password
```

- Adds a CLI view to a superview.
- Multiple views may be added.
- Views may be shared between superviews.

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

Configure Views

```
R1(config)# parser view USER superview
* Mar  1 09:56:26.465 : %PARSER-6-SUPER_VIEW_CREATED: super view 'USER' successfully created.
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
*Mar  1 09:56:33.469: %PARSER-6-SUPER_VIEW_EDIT_ADD: view SHOWVIEW added to superview USER.
R1(config-view)# exit
R1(config)# parser view SUPPORT superview
*Mar  1 09:57:33.825 : %PARSER-6-SUPER_VIEW_CREATED: super view 'SUPPORT' successfully
created.
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIEW
*Mar  1 09:57:45.469: %PARSER-6-SUPER_VIEW_EDIT_ADD: view SHOWVIEW added to superview SUPPORT.
R1(config-view)# view VERIFYVIEW
*Mar  1 09:57:57.077: %PARSER-6-SUPER_VIEW_EDIT_ADD: view VERIFYVIEW added to superview
SUPPORT.
R1(config-view)# exit
R1(config)# parser view JR-ADMIN superview
*Mar  1 09:58:09.993: %PARSER-6-SUPER_VIEW_CREATED: super view 'JR-ADMIN' successfully
created.
R1(config-view)# secret cisco2
R1(config-view)# view SHOWVIEW
*Mar  1 09:58:26.973: %PARSER-6-SUPER_VIEW_EDIT_ADD: view SHOWVIEW added to superview JR-
ADMIN.
R1(config-view)# view VERIFYVIEW
*Mar  1 09:58:31.817: %PARSER-6-SUPER_VIEW_EDIT_ADD: view VERIFYVIEW added to superview JR-
ADMIN.
R1(config-view)# view REBOOTVIEW
*Mar  1 09:58:39.669: %PARSER-6-SUPER_VIEW_EDIT_ADD: view REBOOTVIEW added to superview JR-
ADMIN.
R1(config-view)# exit
```

Display Views

```
R1# show running-config

<output omitted>

!
parser view SUPPORT superview
 secret 5 $1$Vp1O$BBB1N68Z2ekr/aLHledts.
 view SHOWVIEW
 view VERIFYVIEW
!
parser view USER superview
 secret 5 $1$E4k5$ukHyfYP7dHOC48N8pxm4s/
 view SHOWVIEW
!
parser view JR-ADMIN superview
 secret 5 $1$8kx2$rbAe/ji220OmQ1yw.568g0
 view SHOWVIEW
 view VERIFYVIEW
 view REBOOTVIEW
!
```

Verify the USER View

```
R1# enable view USER
Password:
*Mar  1 09:59:46.197: %PARSER-6-VIEW_SWITCH: successfully set to view 'USER'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  show    Show running system information

R1#
R1# show ?
  flash:   display information about flash: file system
  version  System hardware and software status

R1#
```

Verify the SUPPORT View

```
R1# enable view SUPPORT
Password:
*Mar  1 10:00:11.353: %PARSER-6-VIEW_SWITCH: successfully set to view 'SUPPORT'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  show    Show running system information

R1#
```

Verify the JR-ADMIN View

```
R1# enable view JR-ADMIN
Password:
*Mar  1 10:00:28.365: %PARSER-6-VIEW_SWITCH: successfully set to view 'JR-ADMIN'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  reload  Halt and perform a cold restart
  show    Show running system information

R1#
```

Role-Based CLI Monitoring

- When monitoring role-based CLI, use the command **`show parser view`** to display information about the view that the user is currently In (but note that the command must be available in the current view!).
  - The **`all`** keyword displays information for all configured views.
  - The **`all`** keyword is available only to root users.
  - However, the keyword can be configured by a user in root view to be available for users in any CLI view.
- To display debug messages for all views, use the **`debug parser view`** command in privileged EXEC mode.

Verify All Views

```
R1# show parser view
No view is active ! Currently in Privilege Level Context
R1#
R1# enable view
Password:
*Mar  1 10:38:56.233: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1#
R1# show parser view
Current view is 'root'
R1#
R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 SUPPORT *
 USER *
 JR-ADMIN *
 ADMIN *
-------(*) represent superview-------
R1#
```

Resilient Configuration Feature

- If a router is compromised, there is a risk that the configuration and the operating system image can be erased.
  - Availability threat (downtime)
- Need to secure the primary bootset.
  - Configuration file and the running IOS image
- SCP Note:
  - In addition to the Resilient Configuration Feature, configuration and image files can be copied securely to another device using the secure copy program (SCP).
  - Provides a secure and authenticated method for copying router configuration or router image files between devices.
  - Relies on Secure Shell (SSH).

Resilient Configuration Feature

- The **Cisco IOS Resilient Configuration** feature enables a router to secure and maintain a working copy of the running image and configuration files.
  - Speeds up the recovery process.
  - Files are stored locally.
  - Feature can be disabled through a console session.

Securing Configuration Files

- To enable Cisco IOS image resilience, use the command:

```
Router(config)# secure boot-image
```

- To store a secure copy of the primary bootset in persistent storage, use the command:

```
Router(config)# secure boot-config
```

```
R1(config)# secure boot-image
R1(config)# secure boot-config
```

Resilient Configuration Feature Verification

- To display the status of the configuration resilience and the primary bootset filename, use the command:

```
R1# show secure bootset

IOS resilience router id JMX0704L5GH

IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2005
Secure archive slot0:c3745-js2-mz type is image (elf) []
file size is 25469248 bytes, run size is 25634900 bytes
Runnable image, entry point 0x80008000, run from ram

IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16
2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config configuration
archive size 1059 bytes
```

Secure Configuration Files Recovery

- If a router is compromised, you have to reload it to start the recovery procedure.
  - Reloading is not always necessary and may depend on the circumstances.
- `rommon 1 >`
  - Use the **`dir`** and **`boot`** commands to list the contents of the device with secure bootset and to boot the router using the secure bootset image.

```
dir [filesystem:]
boot [partition-number:][filename]
```

Secure Configuration Files Recovery

- After the router boots and if the startup configuration was deleted, the router prompts you for interactive configuration input.
  - Decline to enter an interactive configuration

```
Router(config)# secure boot-config [restore filename]
```

- Use the **secure boot-config restore** command to recover the secured startup configuration.

Secure Configuration Files Recovery

```
rommon 1 > dir slot0:
rommon 2 > boot slot0:c3745-js2-mz
....
Router(config)# secure boot-config restore slot0:RESCUE-CFG
Router# copy slot0:RESCUE-CFG running-config
```

Secure Configuration Files Recovery

```
Router# dir flash:
Directory of flash:/

    1  -rw-    23587052   Jan 9 2010 17:16:58 +00:00  c181x-advipservicesk9-mz.124-24.T.bin
    2  -rw-         600  Sep 26 2010 07:28:12 +00:00  vlan.dat

128237568 bytes total (104644608 bytes free)
Router# dir nvram:
Directory of nvram:/

  189  -rw-        1396                     startup-config
  190  ----          24                     private-config
  191  -rw-        1396                     underlying-config
    1  -rw-           0                     ifIndex-table
    2  -rw-         593                     IOS-Self-Sig#3401.cer
    3  ----          32                     persistent-data

<output omitted>
```

Secure Configuration Files Recovery

- Secure the IOS image.
- Secure the startup-configuration file.

```
R1# config t
R1(config)# secure boot-image
R1(config)#
%IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE: Successfully secured running image
R1(config)# secure boot-config
R1(config)#
%IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully secured config archive
[flash:.runcfg-20101017-020040.ar]
```

Secure Configuration Files Recovery

- Verify the IOS resiliency configuration.

```
R1# show secure bootset
IOS resilience router id FHK110913UQ

IOS image resilience version 12.4 activated at 02:00:30 UTC Sun Oct 17 2010
Secure archive flash:c181x-advipservicesk9-mz.124-24.T.bin type is image (elf) []
  file size is 23587052 bytes, run size is 23752654 bytes
  Runnable image, entry point 0x80012000, run from ram

IOS configuration resilience version 12.4 activated at 02:00:41 UTC Sun Oct 17
2010
Secure archive flash:.runcfg-20101017-020040.ar type is config
configuration archive size 1544 bytes
```

Secure Configuration Files Recovery

- Verify flash to ensure that IOS image file is now hidden.

```
R1# dir flash:
Directory of flash:/

2  -rw-          600  Sep 26 2010 07:28:12 +00:00  vlan.dat

128237568 bytes total (104636416 bytes free)
```

Test Secure Bootset Config

- Verify the configuration by erasing the startup-config and reloading the router.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
R1# show startup-config
startup-config is not present
R1# reload

System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
...
Router> enable
Router# show secure bootset
%IOS image and configuration resilience is not active
```

Test Secure Bootset Config

- Extract the backup startup config file from the secure archive and save it to flash.
- Replace the current running configuration with the archive.

```
Router# config t
Router(config)# secure boot-config restore flash:archived-config
ios resilience:configuration successfully restored as flash:archived-config
Router(config)# ^C
Router# configure replace flash:archived-config
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: y
Total number of passes: 1
Rollback Done

R1# copy run start
```

Test Secure IOS Recovery

- To test that the secure boot image feature works, format flash.

```
R1# format flash:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "flash:".  Continue? [confirm]
Writing Monlib sectors...
Monlib write complete

Format: All system sectors written. OK...

Format: Total sectors in formatted partition: 250848
Format: Total bytes in formatted partition: 128434176
Format: Operation completed successfully.

Format of flash: complete
R1#
```

Test Secure IOS Recovery

- Verify that flash is erased and reload the router.

```
R1# dir
Directory of flash:/

No files in directory

128237568 bytes total (104640512 bytes free)
Router# reload
Proceed with reload? [confirm]

*Oct 17 02:37:37.127: %SYS-5-RELOAD: Reload requested  by console. Reload Reason
: Reload Command.
```

Test Secure IOS Recovery

- The router boots up using the secured IOS image.

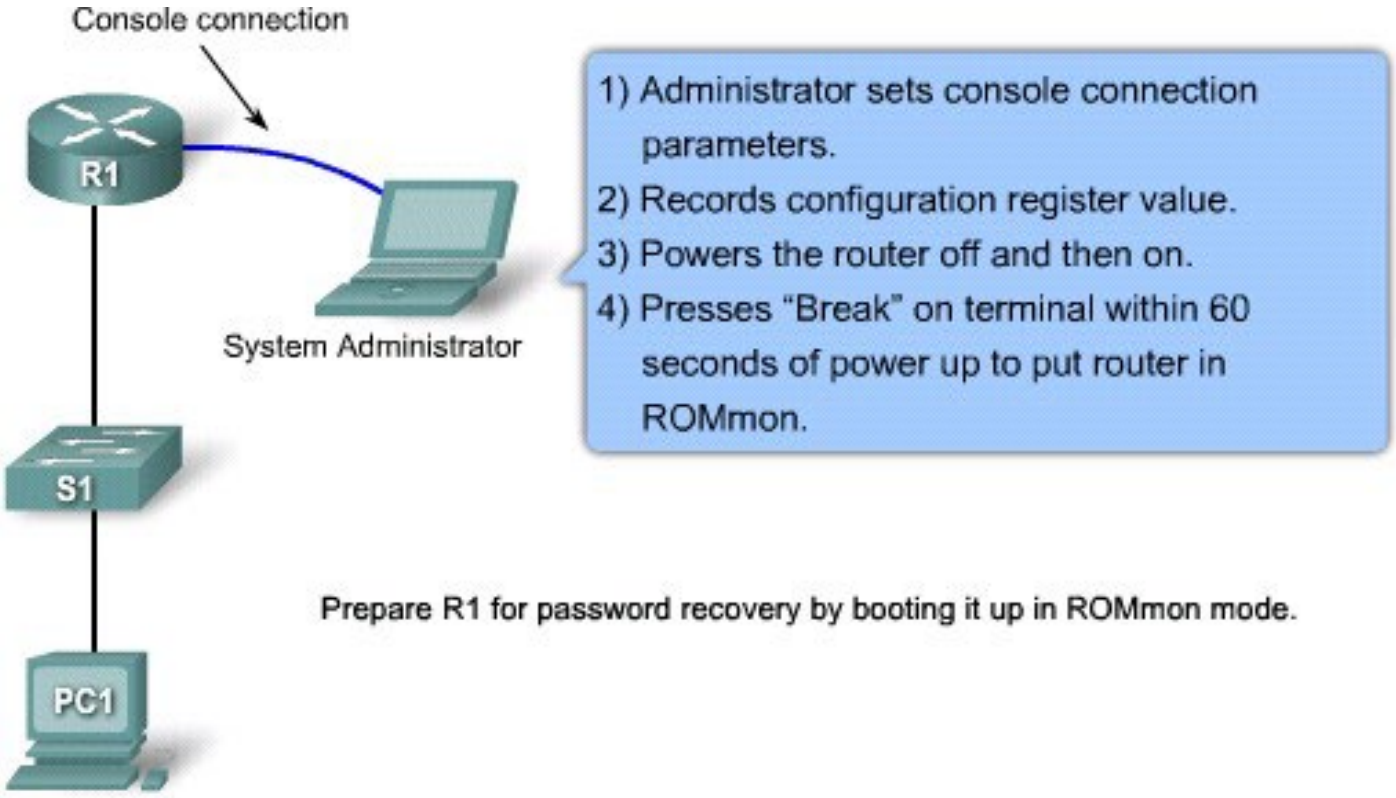
```
...
cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, C181X Software (C181X-ADVIPSERVICESK9-M), Version 12.4(24)T,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Thu 26-Feb-09 03:22 by prod_rel_team
...
R1> enable
Password:
```

Password Recovery

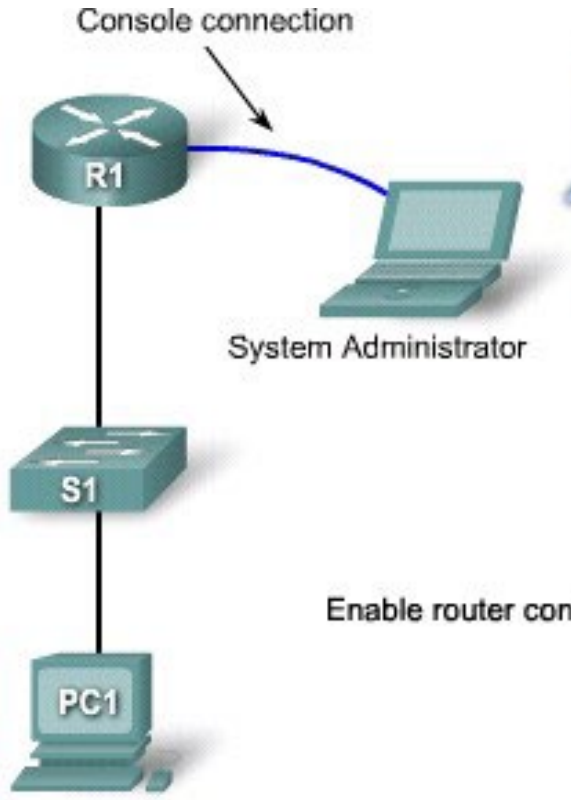
- In the event that a router is compromised or needs to be recovered from a misconfigured password, an administrator must understand password recovery procedures.
- For security reasons, password recovery requires the administrator to have physical access to the router through a console cable.

Password Recovery



Prepare Device | Bypass Startup | Access NVRAM | Reset Passwords

Password Recovery

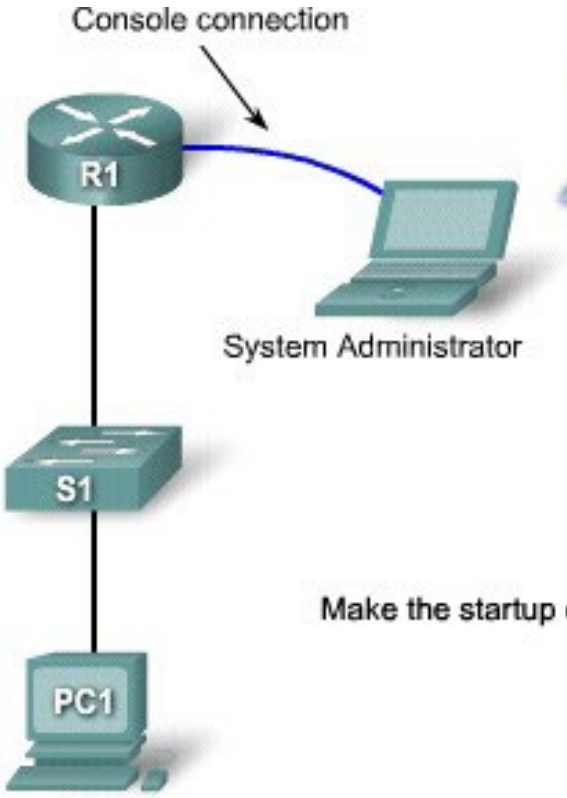


5) Change the config register setting.
6) Reboot. Ignore saved configuration.
7) Skip the initial setup procedure.
8) Type **`enable`** to get to configuration prompt.

Enable router configuration, but bypass the existing startup configuration.

Prepare Device | **Bypass Startup** | Access NVRAM | Reset Passwords

Password Recovery

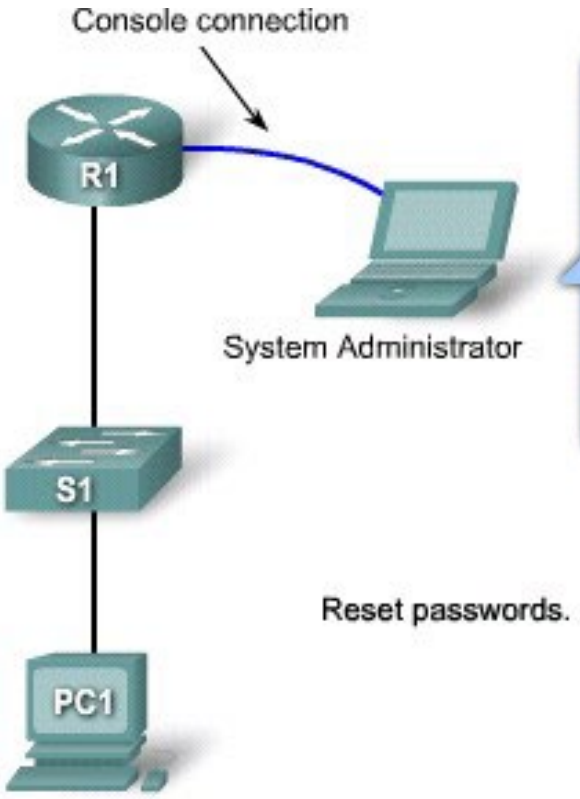


9) Copy the startup configuration from NVRAM to the running configuration in RAM.
10) View passwords by running the **`show running-config`** command.

Make the startup configuration available for viewing.

Prepare Device | Bypass Startup | Access NVRAM | Reset Passwords

Password Recovery



11) Enable global configuration mode.
12) Set a new secret password.
13) Issue `no shutdown` to every operational interface on the router.
14) Set the location of the configuration register.
15) Exit configuration mode.
16) Commit the changes.

Reset passwords.

Prepare Device | Bypass Startup | Access NVRAM | Reset Passwords

Protecting Line Access - Console

- Router access should be protected through the console, auxiliary, and vty lines / ports.
- By default, the Cisco router console ports allow a hard BREAK signal (within 60 seconds of a reboot) to interrupt the normal boot sequence and give the console user complete control of the router.

`no password-recovery` Command

- The **`no service password-recovery`** can be used to disable the HARD BREAK sequence.
  - The command is a hidden Cisco IOS command.
- CAUTION:
  - All access to the ROMMON will be disabled.
  - To repair the router, you must obtain a new Cisco IOS image on a Flash SIMM, or on a PCMCIA card (3600 only) or return the router to Cisco.
- **DO NOT USE THIS COMMAND IN OUR LAB!!!**

no password-recovery Command

```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)
```

```
R1# sho run
Building configuration...

Current configuration : 836 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service password-recovery
```

```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x8000f000, size: 0xcb80
```