Securing Network Devices

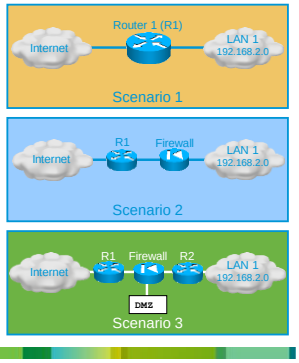
Cisco Integrated Services Routers G2

- Cisco has a new Series of 2nd Generation Routers.
- G2 ISRs have integrated Gigabit Ethernet interfaces.

http://www.cisco.com/en/US/products/ps10906/Products_Sub_Category_Home.html#

Enforcing Perimeter Security Policy

- Routers are used to secure the network perimeter.
- Scenario 1:
  - The router protects the LAN.
- Scenario 2:
  - The router screens traffic before a firewall (PIX/ASA).
- Scenario 3:
  - The zone directly connected to the firewall is called a DMZ.
  - Internet-accessible servers are located in the DMZ.



Three Areas of Router Security

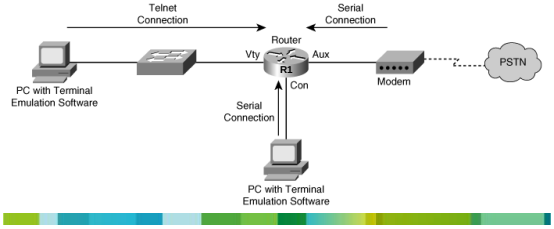
- Physical security
  - Secure infrastructure equipment in a locked room that:
    - Is accessible only to authorized personnel.
    - Is free of electrostatic or magnetic interference.
    - Has fire suppression.
    - Has controls for temperature and humidity.
  - Install an uninterruptible power supply (UPS) and keep spare components available to reduce the possibility of a DoS attack from power loss to the building.

Three Areas of Router Security

- Operating system
  - Configure the router with the maximum amount of memory possible.
    - Helps protect it from some DoS attacks.
  - Use the latest stable version of the operating system that meets the feature requirements of the network.
  - Keep a secure copy of the router operating system image and router configuration file as a backup.

Three Areas of Router Security

- Router hardening
  - Secure administrative control to ensure that only authorized personnel have access and that their level of access is controlled.
  - Disable unused ports and interfaces to reduce the number of ways a device can be accessed.
  - Disable unnecessary services that can be used by an attacker to gather information or for exploitation.



Secure Administrative Access

- Restrict device accessibility
  - Limit the accessible ports, restrict the permitted communicators, and restrict the permitted methods of access.
- Log and account for all access
  - For auditing purposes, record anyone who accesses a device, including what occurs and when.
- Authenticate access
  - Ensure that access is granted only to authenticated users, groups, and services.
  - Limit the number of failed login attempts and the time between logins.

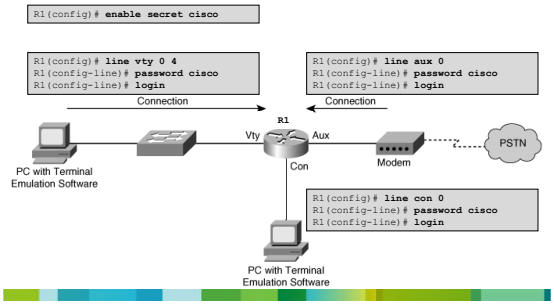
Secure Administrative Access

- Authorize actions
  - Restrict the actions and views permitted by any particular user, group, or service.
- Present Legal Notification
  - Display a legal notice, developed in conjunction with company legal counsel, for interactive sessions.
- Ensure the confidentiality of data
  - Protect locally stored sensitive data from viewing and copying.
  - Consider the vulnerability of data in transit over a communication channel to sniffing, session hijacking, and man-in-the-middle (MITM) attacks.

Secure Administrative Access

Cisco Router Passwords

- All routers need a locally configured password for privileged access and other access.



Cisco Router Passwords

- To steal passwords, attackers:
  - Shoulder surf.
  - Guess passwords based on the user's personal information.
  - Sniff TFTP packets containing plaintext configuration files.
  - Use readily available brute force attack tools such as L0phtCrack or Cain & Abel.
- Strong passwords are the primary defense against unauthorized access to a router!

Strong Passwords

- Passwords should NOT use dictionary words
  - Dictionary words are vulnerable to dictionary attacks.
- Passwords may include the following:
  - Any alphanumeric character.
  - A mix of uppercase and lowercase characters.
  - Symbols and spaces.
  - A combination of letters, numbers, and symbols.

Note:

- Password-leading spaces are ignored, but all spaces after the first character are NOT ignored.

Strong Passwords

- Change passwords frequently.
  - Implement a policy defining when and how often the passwords must be changed.
  - Limits the window of opportunity for a hacker to crack a password.
  - Limits the window of exposure after a password has been cracked.
- Local rules can make passwords even safer.

Passphrases

- One well known method of creating strong passwords is to use **passphrases.**
  - Basically a sentence / phrase that serves as a more secure password.
  - Use a sentence, quote from a book, or song lyric that you can easily remember as the basis of the strong password or pass phrase.
- For example:
  - "My favorite spy is James Bond 007." = **MfsiJB007**.
  - "It was the best of times, it was the worst of times." = **Iwtbotiwtwot**.
  - "Fly me to the moon. And let me play among the stars." = **FmttmAlmpats**.

Password Protection Guidelines

- Use a password length of 10 or more characters. The longer, the better.
- Make passwords complex by including a mix of UPPERCASE and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
- Deliberately misspell a password.
  - For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Change passwords often so if a password is unknowingly compromised, the window of opportunity for the attacker to use the password is limited.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

Cisco Router Passwords

- To increase the security of passwords, the following Cisco IOS commands should be utilized:
  - Enforce minimum password length: **`security passwords min-length`**.
  - Disable unattended connections: **`exec-timeout`**.
  - Encrypt config file passwords: **`service password-encryption`**.

Enforce Minimum Password Lengths

- Make passwords lengthy.
  - IOS 12.3 and later passwords can be 0 to 16 characters in length.
  - The best practice is to have a minimum of 10 characters.
- To enforce the minimum length use the global command:
  - **security passwords min-length** *length*
- The command affects all "new" router passwords.
  - Existing router passwords are unaffected.
- Any attempt to create a new password that is less than the specified length fails and results in an "Password too short" error message.

Disable Unattended Connections

- By default, an administrative interface stays active and logged in for 10 minutes after the last session activity.
  - After that, the interface times out and logs out of the session.
- The timer can be adjusted using the **exec-timeout** command in line configuration mode for each of the line types that are used.
  - **exec-timeout** *minutes seconds*

Note:

- **exec-timeout 0 0** means that there will be no timeout and the session will stay active for an unlimited time.
  - Great for Labs …
  - Bad in production networks!
  - Never set the value to 0!

Disable Unattended Connections

- Default time is 10 minutes.
- Terminates an unattended connection (console or vty).
- Provides additional level of security if an administrator walks away from an active console session.

```
Router(config-line)#
exec-timeout minutes [seconds]
```

  - To terminate an unattended console connection after 3 minutes and 30 seconds:

```
Sudbury(config)# line console 0
Sudbury(config-line)# exec-timeout 3 30
```

  - To disable the exec process on the line:

```
Sudbury(config)# line aux 0
Sudbury(config-line)# no exec-timeout
```


Encrypt All Passwords

- Encrypt all passwords in the router configuration file.

```
Router(config)#
service password-encryption
```

```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config
enable password 7 06020026144A061E
!
line con 0
 password 7 094F471A1A0A
login
!
line aux 0
 password 7 01100F175804575D72
 login
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 login
```

Securing Local Database Passwords

- Secure the local database passwords.
  - Traditional user configuration with plaintext password.

```
username name password {[0] password | 7 hidden-password}
```

  - Use MD5 hashing for strong password protection.
  - More secure than the type 7 encryption.

```
username name secret {[0] password | encrypted-secret}
```


Securing Local Database Passwords

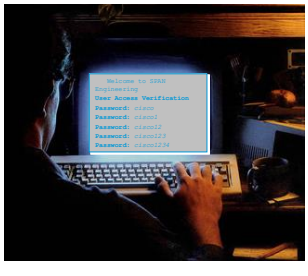
```
R1# conf t
R1(config)# username JR-ADMIN password letmein
% Password too short - must be at least 10 characters. Password configuration
failed
R1(config)# username JR-ADMIN password cisco12345
R1(config)# username ADMIN secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
```

```
R1# show run | include username
username JR-ADMIN password 7 060506324F41584B564347
username ADMIN secret 5 $1$G3oQ$hEvsd5iz76WJuSJvtzs8I0
R1#
```

```
R1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: ADMIN
Password:
R1>
```


Secure Virtual Logins

- To improve security for virtual login connections, the login process should be configured with specific parameters:
  - Implement delays between successive login attempts.
  - Enable login shutdown if DoS attacks are suspected.
  - Generate system logging messages for login detection.



Disable Login for Excessive Attempts

```
R1# configure terminal
R1(config)# username ADMIN secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config)# exit
R1(config)# login block-for 120 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)# exit
```

- In this sample config, if more than 5 login failures occur within 60 seconds, then all logins will be disabled for 120 seconds.
  - This command must be issued before any other login command can be used.
  - The command also helps provide DoS detection and prevention.
- The PERMIT-ADMIN commands exempt administrative stations from the disabled login.
  - If not configured, all login requests will be denied during the Quiet-Mode.

Verify Login Security

```
R1# show login
     A login delay of 10 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or less,
     logins will be disabled for 120 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 5 seconds.
         Login failures for current window: 4.
     Total login failures: 4.
```

- In this example, the **`login block-for`** command was configured to block login hosts for 120 seconds if more than 5 login requests fail within 60 seconds.

Verify Login Security When in Quiet Mode

```
R1#
*Dec 10 15:38:54.455: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching
failures is 12 secs, [user: admin] [Source: 10.10.10.10] [localport: 23] [Reason:
Login Authentication Failed - BadUser] [ACL: PERMIT-ADMIN] at 15:38:54 UTC Wed Dec
10 2008

R1# show login
     A login delay of 10 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or less,
     logins will be disabled for 120 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 105 seconds.
     Restricted logins filtered by applied ACL PERMIT-ADMIN.

R1#
```

- In this example, a 6th failed attempt at logging has occurred.
  - A log message is initiated at the console stating that the router is in Quiet-Mode.
  - All login attempts made using Telnet, SSH, and HTTP are denied except as specified by the PERMIT-ADMIN ACL.

Verify Login Security When in Quiet Mode

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username        SourceIPAddr    lPort Count TimeStamp
admin           1.1.2.1         23    5     15:38:54 UTC Wed Dec 10 2011
Admin           10.10.10.10     23    13    15:58:43 UTC Wed Dec 10 2011
admin           10.10.10.10     23    3     15:57:14 UTC Wed Dec 10 2011
cisco           10.10.10.10     23    1     15:57:21 UTC Wed Dec 10 2011

R1#
```

- In this example, the command identifies the number of failures, usernames tried, and offending IP addresses with a timestamp added to each unsuccessful attempt.

Provide Legal Notification

- Banner messages should be used to warn would-be intruders that they are not welcome on your network.
- Banners are important, especially from a legal perspective.
  - Intruders have been known to win court cases because they did not encounter appropriate warning messages.
  - Choosing what to place in banner messages is extremely important and should be reviewed by legal counsel before being implemented.
  - Never use the word “welcome” or any other familiar or similar greeting that may be misconstrued as an invitation to use the network.

Configuring Banner Messages

- Specify what is “proper use” of the system.
- Specify that the system is being monitored.
- Specify that privacy should not be expected when using this system.
- Do not use the word “welcome.”
- Have legal department review the content of the message.

```
Router(config)#
banner {exec | incoming | login | motd | slip-ppp} d message d
```


Protecting vty Line Access #1

- By default, Cisco routers do NOT have any line-level passwords configured for vty lines.
  - Passwords must be configured for all of the vty lines on the router.
  - Remember that more vty lines can be added to the router.
- If password checking is enabled (i.e., the **login** command), a vty password must also be configured before attempting to access the router using Telnet.
  - If a vty password is NOT configured and password checking is enabled for vty, an error message similar to the following will be produced:

```
Telnet 10.0.1.2
Trying 10.0.1.2 …. open
Password required, but none set
[Connection to 10.0.1.2 closed by foreign host]
```


Protecting vty Line Access #2

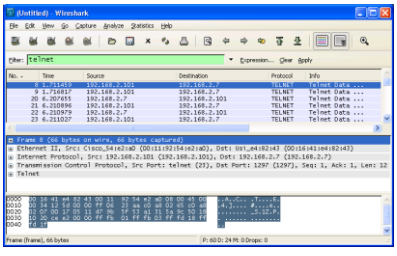
- If an enable mode password is NOT set for the router, privileged-EXEC mode can NOT be accessed using Telnet.
- Always use the **enable secret** *password* command to set the enable password.
  - Never use the **enable password** command!

Protecting vty Line Access #3

- Telnet access should be limited only to specified administrative hosts using ACLs:
  - Allows Telnet access from specific hosts only.
  - Implicitly or explicitly blocks access from untrusted hosts.
  - Tie the ACL to the vty lines using the **access-class** command.
- For example:

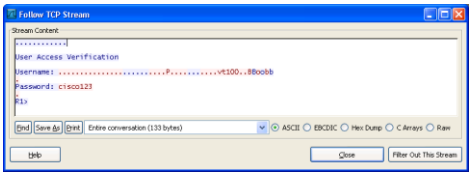
```
R1(config)# access-list 30 permit 10.0.1.1 0.0.0.0
R1(config)# line vty 0 4
R1(config-line)# access-class 30 in
```

Sniffing a Telnet Password



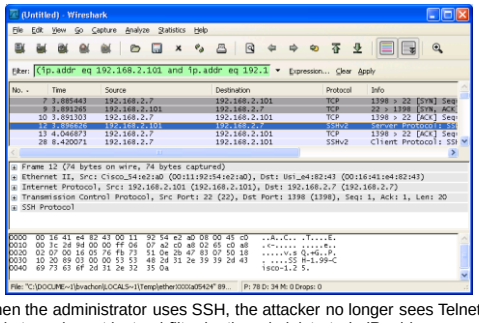
- An attacker is capturing packets using Wireshark on a local subnet.
- The attacker is interested in TCP Telnet streams and notices that the administrator's IP address (192.168.2.7) has initiated a Telnet session to a device.

Follow the TCP Stream



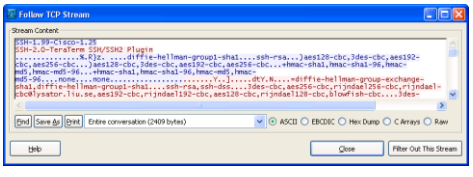
- By following the TCP Telnet stream, the attacker has captured the administrator's username (Bob) and password (cisco123).

Configure SSH



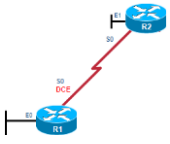
- When the administrator uses SSH, the attacker no longer sees Telnet packets and must instead filter by the administrator's IP address.

Follow the TCP Stream



- When following the stream of data, the attacker only sees TCP and SSH packets which reveal useless encrypted information.

Configuring SSH



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

```
R1# conf t
R1(config)# ip domain-name span.com
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
```

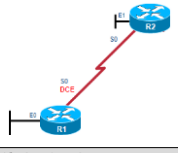
Optional SSH Features

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

Optional SSH Features

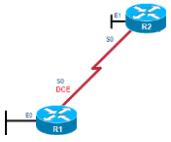
- **SSH Versions:**
  - Cisco IOS Release 12.1(1)T and later supports SSHv1.
  - Cisco IOS Release 12.3(4)T and later supports both SSHv1 and SSHv2 (compatibility mode).
  - To change versions, use the **ip ssh version {1 | 2}** global command.
- **Number of authentication retries:**
  - By default, 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# conf t
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>
```

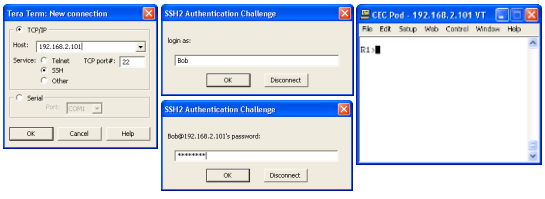
1 There are no current SSH sessions ongoing with R1.

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

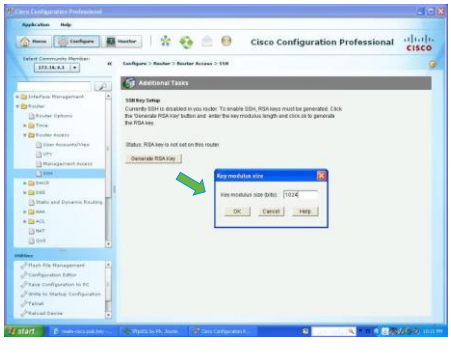
3 There is an incoming and outgoing SSHv2 session with user Bob.

```
R1# sho 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#
```

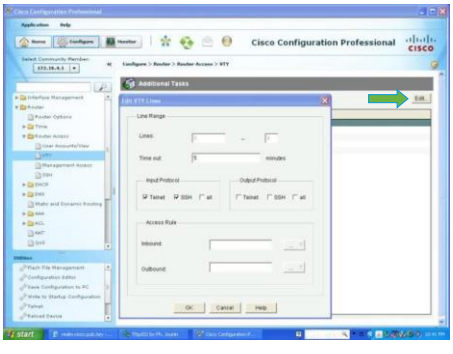
Host-to-Router SSH



Configuring SSH Using CCP



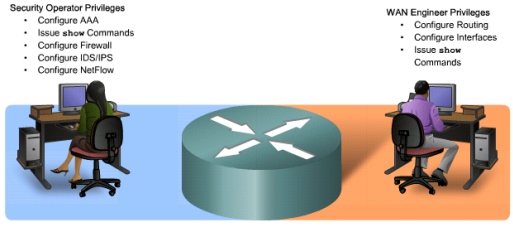
Configuring SSH Using CCP



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 has all of the regular privileged EXEC commands.

```
R1# conf t
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.
  - Notice the prompt indicates Level 1 (R1>).
  - 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.
  - Notice now the user can **ping** but cannot use the **reload** command.

```
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

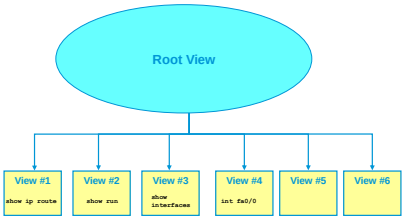
- No access control to specific interfaces, ports, logical interfaces, and slots on a router.
- Commands available at lower privilege levels are always executable at higher levels.
- Commands specifically set on a higher privilege level are not available for lower privileged users.
- Assigning a command 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) 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.
- Adds commands or interfaces to a view.

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

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

```
R1(config)# parser view MONITOR-VIEW
R1(config-view)# password cisco
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# config t
R1(config)# username Bob view FIRST password cisco123
```

Another Sample Config

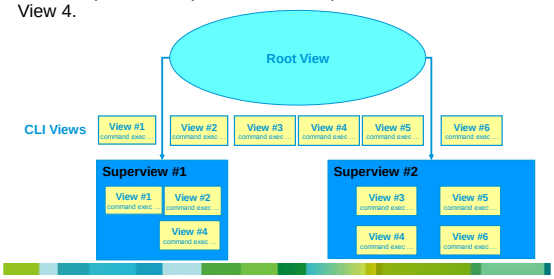
```
R1(config)# parser view SHOWVIEW
*Mar  1 09:54:54.873: %PARSER-6-VIEW_CREATED: view 'SHOWVIEW' successfully
created.
R1(config-view)# secret cisco
R1(config-view)# commands exec include show version
R1(config-view)# exit
R1(config)# parser view VERIFYVIEW
*Mar  1 09:55:24.813: %PARSER-6-VIEW_CREATED: 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$8njLecwTaLAc0UuWol/Fv0
 commands exec include show version
 commands exec include show
!
parser view VERIFYVIEW
 secret 5 $1$d08J$1zOYSI4WainGxkn0Hu71P1
 commands exec include ping
!
parser view REBOOTVIEW
 secret 5 $1$L71Z$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 $1$VplO$BBBlN68Z2ekr/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/ji220OmQlyw.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.
  - 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 Secure Copy (SCP).
  - Provides a secure and authenticated method for copying router configuration or router image files between devices.
  - Relies on Secure Shell (SSH).
  - Configuration is covered in Chapter 9.

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.
- Must enter ROMMON mode.
  - 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.

```
rommon 1 >
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 session.
- Use the **secure boot-config restore** command to recover the secured startup configuration.

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


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

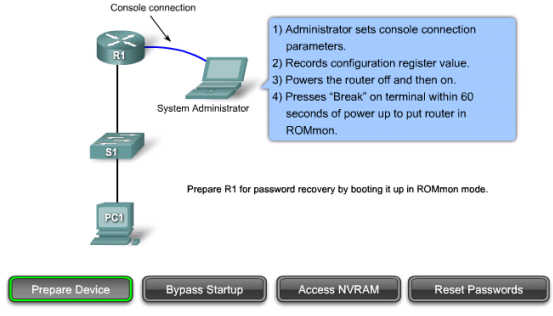
- The router boots up using the secured IOS image.

```
...
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:
```

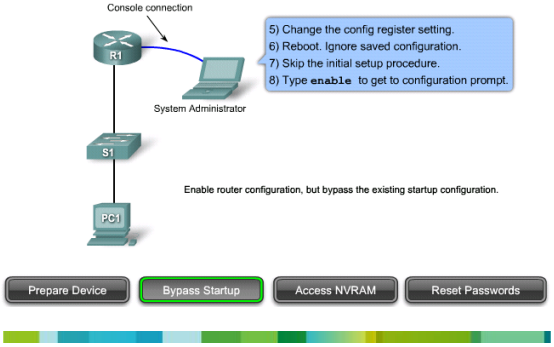
Password Recovery

- 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.

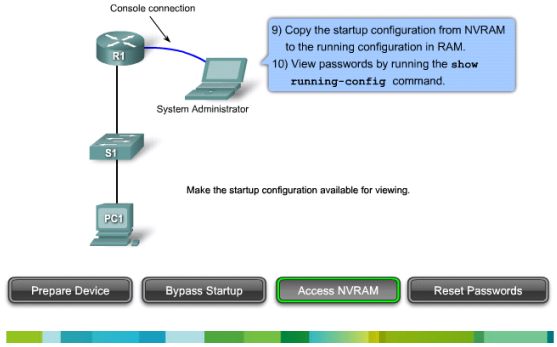
Password Recovery



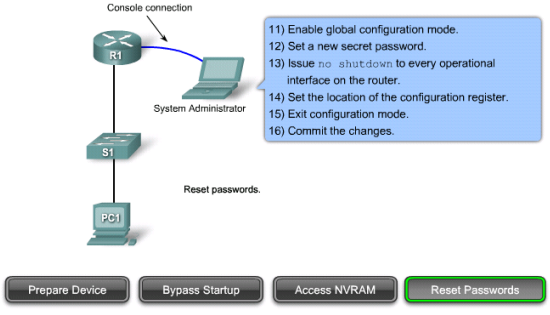
Password Recovery



Password Recovery



Password Recovery



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`** command 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
```

Securing Management and Reporting Features

Management Reporting Considerations

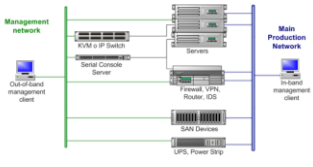
- Configuring logging for a few devices is a fairly simple and straightforward operation.
- Configuring logging for hundreds of devices can be very challenging.

Information Paths

- Information flow between management hosts and the managed devices can take two paths.

Out of Band (OOB):
- Information flows within a network on which **no** production traffic resides.

In-Band:
- Information flows across the enterprise production network or the Internet (or both).



Logging Management Considerations

- Some questions that must be considered when designing an in-band management solution:
  - Which management protocols does each device support?
  - Does the management channel need to be active at all times?
  - Is SNMP necessary?
  - Which are the most important logs?
  - How are important messages separated from routine notifications?
  - How do you prevent tampering with logs?
  - How do you make sure time stamps match?
  - What log data is needed in criminal investigations?
  - How do you deal with the volume of log messages?
  - How do you manage all the devices?
  - How can you track changes when attacks or network failures occur?

In-Band Management Guidelines

- Apply only to devices needing to be managed or monitored.
- Use IPsec when possible.
- Use SSH or SSL instead of Telnet.
- Decide whether the management channel needs to be open at all times.
- Keep clocks on hosts and network devices synchronized.
- Record changes and archive configurations.

OOB Management Guidelines

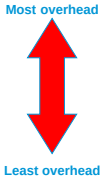
- Provide highest level of security and mitigate the risk of passing insecure management protocols over the production network.
- Keep clocks on hosts and network devices synchronized.
- Record changes and archive configurations.

Implementing Log Messaging for Security

- Routers should be configured to send log messages to one or more of these:
  - Console
  - Terminal lines
  - Memory buffer
  - SNMP Server
  - Syslog Server

Logging Destinations

- Be aware that the logging destination used affects system overhead.
  - Logging to the **console**.
  - Logging to **VTY**.
  - Logging to a **Syslog Server**.
  - Logging to an internal **buffer**.



Two Components of Syslog Systems

- Syslog server:
  - A host that accepts and processes log messages from one or more syslog clients.
- Syslog client:
  - A host that generates log messages and forwards them to a syslog server.
  - Routers, switches, PIXs, ASAs, APs, servers, …

Syslog Error Message Levels

Highest Level

Level	Keyword	Description	Syslog Definition
0	**emergencies**	System is unusable.	LOG_EMERG
1	**alerts**	Immediate action is needed.	LOG_ALERT
2	**critical**	Critical conditions exist.	LOG_CRIT
3	**errors**	Error conditions exist.	LOG_ERR
4	**warnings**	Warning conditions exist.	LOG_WARNING
5	**notification**	Normal but significant condition.	LOG_NOTICE
6	**informational**	Informational messages only.	LOG_INFO
7	**debugging**	Debugging messages.	LOG_DEBUG

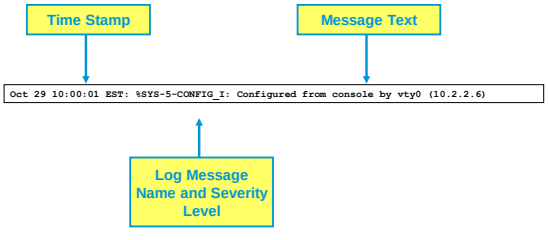
Lowest Level

- By default, Severity level 7 (debugging) messages are sent to the router's console port (line con0).
- Note: Level varies by platform and IOS release.

Cisco Log Severity Levels

Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, hard device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Conditions that are not error conditions but should possibly be addressed	Interface changed state, up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information that is normally used only when debugging	Packet type invalid

Log Message Format



Note: The log message name is not the same as a severity level name.

Configuring Syslog Step 1

1. Set the destination logging host.
   - You can specify the IP address or the DNS name.

```
Router(config)#
logging host [host-name | ip-address]
```

Parameter	Description
host-name	The name of the host you want to use as a syslog server
ip-address	The IP address of the host you want to use as a syslog server

Configuring Syslog Step 2

2. (Optional) Set the log severity (trap) level.

```
Router(config)#
logging trap level
```

Parameter	Description
level	Limits the logging of messages to the syslog servers to a specified level. You can enter the level number (0 to 7) or level name.

Configuring Syslog Step 3

3. (Optional) Set the source interface.
   - Specifies that syslog packets contain the IP or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

```
Router(config)#
logging source-interface interface-type interface-number
```

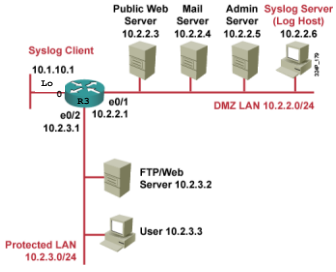
Parameter	Description
interface-type	The interface type (for example, FastEthernet)
interface-number	The interface number (for example, 0/1)

Configuring Syslog Step 4

4. Enable logging
   - You can enable or disable logging individually:
     - **[no] logging buffered**
     - **[no] logging monitor**
   - However, if the **no logging** on command is configured, no messages will be sent to these destinations.

```
Router(config)#
logging on
```

Syslog Implementation Example




```
R3(config)# logging 10.2.2.6
R3(config)# logging trap informational
R3(config)# logging source-interface loopback 0
R3(config)# logging on
```


VTY Monitor Logging

- The VTY monitoring option is the most practical method for viewing logging events in real time.
- To view system messages over a VTY session (line vty 0 - 4), **`logging monitor`** must be configured.
- To enable monitor logging, use the configuration command **`logging monitor [`***`severity`***`]`**.

VTY Monitor Logging

- Hmmm … I'm Telnetted into a router and entered **`debug ip packet`** but don't see any output. Why?
- You have to enter the enable exec command **`terminal monitor`** to activate logging and see console message output to the vty.

VTY Monitor Logging

- Telnet from another host and use the EXEC command **`terminal monitor`** to view the output.

```
R3(config)# logging monitor
R3(config)# logging monitor error
```

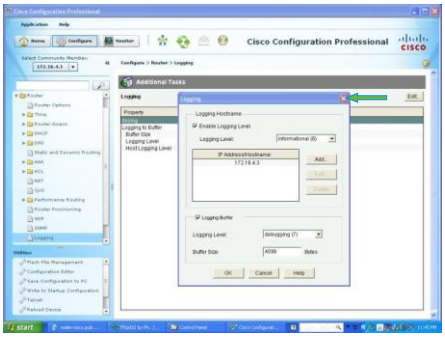
VTY Monitor Logging Tip

- It is recommended to establish two VTY sessions:
  - One for displaying event reporting data.
  - The other for command execution.
- Why?
  - Once terminal monitoring is enabled, it cannot be disabled on that VTY session.
  - A large amount of logging data can be generated, obscuring the VTY with logging output and making command entry quite difficult at times.

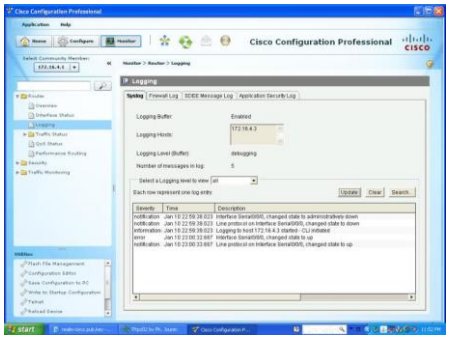
`logging synchronous`

- The **`logging synchronous`** line configuration command also affects the display of messages to the console.
- When enabled, messages will appear only after the user types a carriage return.
- Without the this command, console messages displayed can interfere with command line entry.

Configuring Logging in CCP



Configuring Logging in CCP



Configuring NTP

Understanding NTP

- "Time has been invented in the universe so that everything would not happen at once."
  - The NTP FAQ and HOWTO - http://www.ntp.org/ntpfaq/
- Many features in a computer network depend on time synchronization:
  - For accurate time information in syslog messages.
  - Certificate-based authentication in VPNs.
  - ACLs with time range configuration.

System Clock

- The heart of the router time service is the software-based system clock.
  - This clock keeps track of time from the moment the system starts.
- The system clock can be set from a number of sources and can be used to distribute the current time through various mechanisms to other systems.
  - When a router with a system calendar is initialized or rebooted, the system clock is set based on the time in the internal battery-powered system calendar.
- The system clock can then be set:
  - Manually using the **`set clock`** privileged EXEC command.
  - Automatically using the Network Time Protocol (NTP).
- NTP is an Internet protocol used to synchronize the clocks of network connected devices to some time reference.
  - NTP is an Internet standard protocol currently at v3 and specified in RFC 1305.

NTP

- NTP is designed to time-synchronize a network.
  - NTP runs over UDP.
- An NTP network usually obtains the time from an authoritative time source, such as a radio clock or an atomic clock.
  - NTP then distributes this time across the network.
  - NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within 1 mSec of one another.
- Cisco devices support specifications for NTP v3 (RFC 1305).
  - NTP v4 is under development but NTP v3 is the Internet standard.
- NTP services are enabled on all interfaces by default.
  - To disable NTP on a specific interface, use the **`ntp disable`** command in the interface configuration mode.

Configuring an NTP Master and Client

- To configure a router as the authoritative time source, use the **ntp master** command in global configuration mode.
- To configure a router as an NTP client, either:
  - Create an association to a server using the **ntp server** command.
  - Configure the router to listen to NTP broadcast packets using the **ntp broadcast client** command.

Identifying the NTP Server

- Although the router can be configured with either a peer or a server association, NTP clients are typically configured with a server association (meaning that only this system will synchronize to the other system, and not vice versa).
- To allow the software clock to be synchronized by an NTP time server, use the **ntp server** command in global configuration mode.

```
Router(config)#
ntp server {ip-address | hostname} [version number] [key keyid] [source interface]
[prefer]
```


Configuring NTP Associations

- NTP broadcast client:
  - In addition to or instead of creating unicast NTP associations, the system can be configured to listen to broadcast packets on an interface-by-interface basis.
- To do this, use the **ntp broadcast client** command in interface configuration mode.

```
Router(config-if)#
ntp broadcast client
```


NTP Security

- The time that a machine keeps is a critical resource, so the security features of NTP should be used to avoid the accidental or malicious setting of incorrect time.
- Two mechanisms are available:
  - ACL-based restriction scheme
  - Encrypted authentication

NTP Authentication Commands

Command	Description
ntp authenticate	Enables the NTP authentication feature. If this command is specified, the system will not synchronize to another system unless the other system's NTP messages carry one of the specified authentication keys.
ntp authentication-key *number* **md5** *value*	Defines an authentication key supported by using MD5. The key type md5 is currently the only key type that this command supports. The key value can be any arbitrary string of up to eight characters.
ntp trusted-key *key-number*	Defines trusted authentication keys.

Configuring NTP Authentication

- Enable the authentication feature.

```
Router(config)#
ntp authentication
```

- Define the authentication key to be used for both peer and server associations.

```
Router(config)#
ntp authentication-key key-number md5 value
```

- Define which key is to be trusted.

```
Router(config)#
ntp trusted-key key-number
```


NTP Configuration Example


```
R1(config)# ntp master 5
R1(config)# ntp authentication-key 1 md5 R1-SECRET
R1(config)# ntp peer 209.165.200.225 key 1
```

```
R2(config)# ntp authentication-key 1 md5 R1-SECRET
R2(config)# ntp authentication-key 2 md5 R2-SECRET
R2(config)# ntp trusted-key 1
R2(config)# ntp server 209.165.201.1
R2(config)# interface Fastethernet0/0
R2(config-if)# ntp broadcast
```

```
R3(config)# ntp authentication-key 1 md5 R2-SECRET
R3(config)# ntp trusted-key 1
R3(config)# interface Fastethernet0/1
R3(config-if)# ntp broadcast client
```


Disabling Unused Cisco Router Network Services and Interfaces

Vulnerable Router Services

- Medium size and large networks typically use a firewall appliance (PIX / ASA) behind the perimeter router, which adds security features and performs user authentication and more advanced packet filtering.
- Firewall installations also facilitate the creation of Demilitarized Zones (DMZs), where the firewall 'places' hosts that are commonly accessed from the Internet.

Vulnerable Router Services

- As an alternative, Cisco IOS software can incorporate many firewall features in the perimeter router.
  - Option is valid only for small-to-medium business perimeter security requirements.
- However, Cisco IOS routers run many services that create potential vulnerabilities.
  - To secure an enterprise network, all unneeded router services and interfaces must be disabled.

Unnecessary Services

Router Service	Description	Default	Best Practice
BOOTP server	• This service allows a router to act as a BOOTP server for other routers. • If not required, disable this service.	Enabled	Disable. `no ip bootp server`
Cisco Discovery Protocol (CDP)	• CDP obtains information of neighboring Cisco devices. • If not required, disable this service globally or on a per-interface basis.	Enabled	Disable if not required. **no cdp run**
Configuration auto-loading	• Auto-loading of configuration files from a network server should remain disabled when not in use by the router.	Disabled	Disable if not required. **no service config**
FTP server	• The FTP server enables you to use your router as an FTP server for FTP client requests. • Because this server allows access to certain files in the router Flash memory, this service should be disabled when not required.	Disabled	Disable if not required. Otherwise encrypt traffic within an IPsec tunnel.
TFTP server	• Same as FTP.	Disabled	Disable if not required. Otherwise encrypt traffic within an IPsec tunnel.
Network Time Protocol (NTP) service	• When enabled, the router acts as a time server for other network devices. • If configured insecurely, NTP can be used to corrupt the router clock and potentially the clock of other devices that learn time from the router. • If this service is used, restrict which devices have access to NTP.	Disabled	Disable if not required. Otherwise configure NTPv3 and control access between permitted devices using ACLs.

Unnecessary Services

Router Service	Description	Default	Best Practice
Packet assembler and disassembler (PAD) service	• The PAD service allows access to X.25 PAD commands when forwarding X.25 packets.	Enabled	Disable if not required.

TCP and UDP minor services	• The minor services are provided by small servers (daemons) that run in the router. The services are potentially useful for diagnostics, but are rarely used.	Enabled (pre 11.3)
		Disabled (11.3+)
			Disable if not required.
			`no service tcp-small-servers`
			`no service udp-small-servers`

Maintenance Operation Protocol (MOP) service	• MOP is a Digital Equipment Corporation (DEC) maintenance protocol that should be explicitly disabled when not in use.	Enabled	Disable explicitly if not required.

Commonly Configured Management Services

Service	Description	Default	Best Practice
Simple Network Management Protocol (SNMP)	• The SNMP service allows the router to respond to remote SNMP queries and configuration requests. • If required, restrict which SNMP systems have access to the router SNMP agent and use SNMPv3 whenever possible because version 3 offers secure communication that is not available in earlier versions of SNMP.	Enabled	Disable the service. Otherwise configure SNMPv3.
HTTP configuration and monitoring	• This service allows the router to be monitored or have the router configuration modified from a web browser via an application such as the Cisco Security Device Manager (SDM). You should disable this service if the service is not required. If this service is required, restrict access to the router HTTP service by using access control lists (ACLs).	Device dependent	Disable if not required. Otherwise restrict access using ACLs. `no ip http server`

Domain Name System (DNS)	• By default, Cisco routers broadcast name requests to 255.255.255.255.
	• Restrict this service by disabling DNS when the service is not required.
	• If the DNS lookup service is required, make sure that you set the DNS server address explicitly.
		Client Service – Enabled	Disable if not required. Otherwise explicitly configure the DNS server address.
			`no ip domain-lookup`
			`no ip name-server`

Path Integrity Mechanisms

Path Integrity Mechanisms	Description	Default	Best Practice
ICMP redirects	• ICMP redirects cause the router to send ICMP redirect messages whenever the router is forced to resend a packet through the same interface on which the packet was received. • This information can be used by attackers to redirect packets to an untrusted device.	Enabled	Disable the service.
IP source routing	• The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that a datagram will take toward the datagram's ultimate destination, and generally the route that any reply will take. • These options can be exploited by an attacker to bypass the intended routing path and security of the network. • Also, some older IP implementations do not process source-routed packets properly, and hackers may be able to crash machines that run these implementations by sending datagrams with source routing options.	Enabled	Disable if not required. `no ip source-route`

Probe and Scan Features

Probes and Scan Features	Description	Default	Best Practice

Finger service	• The finger protocol (port 79) can obtain a list of the users who are currently logged into a device.
	• Unauthorized persons can use this information for reconnaissance attacks.
		Enabled	Disable if not required.
			`no ip finger`
			`no service finger`

ICMP unreachable notifications	• ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Cisco routers automatically send ICMP messages.
	• Attackers commonly use three ICMP messages:
	  • Host unreachable
	  • Redirect
	  • Mask Reply
	• Automatic generation of these messages should be disabled on all interfaces, especially interfaces that are connected to untrusted networks.
		Enabled	Disable explicitly on untrusted interfaces.

ICMP mask reply	• When enabled, this service tells the router to respond to ICMP mask requests by sending ICMP mask reply messages that contain the interface IP address mask. • This information can be used to map the network.	Disabled	Disable explicitly on untrusted interfaces.

Terminal Access Security

Terminal Access Security	Description	Default	Best Practice
IP identification service	• The identification protocol (specified in RFC 1413) reports the identity of a TCP connection initiator to the receiving host. • This data can be used by an attacker to gather information about your network	Enabled	Disable.
TCP Keepalives	• TCP keepalives help "clean up" TCP connections where a remote host has rebooted or otherwise stopped processing TCP traffic. • Keepalives should be enabled globally to manage TCP connections and prevent certain DoS attacks.	Disabled	Enable.

ARP Service

Terminal Access Security	Description	Default	Best Practice
Gratuitous ARP	• Gratuitous ARP is the main mechanism that hackers use in ARP poisoning attacks.	Enabled	Disable if not required.
Proxy ARP	• Proxy ARP enables a Cisco router to act as an intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments. • Proxy ARP should be used only between two LAN segments at the same trust level, and only when absolutely necessary to support legacy network architectures.	Enabled	Disable if not required.

IP Directed Broadcasts

IP Directed Broadcasts	Description	Default	Best Practice
IP Directed Broadcasts	• IP directed broadcasts are used in the common and popular smurf DoS attack and other related attacks. • Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. • This technique was used in some old DoS attacks, and the default Cisco IOS configuration is to reject directed broadcasts.	Enabled (pre 12.0) Disabled (12.0+)	Disable if not required.

Disable Unneeded Services

```
Router(config)# no ip bootp server
Router(config)# no cdp run
Router(config)# no ip source-route
Router(config)# no ip classless
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no ip finger
Router(config)# no service finger
Router(config)# no ip http server
Router(config)# no ip name-server
Router(config)# no boot network
Router(config)# no service config
```


IP Classless Routing

- By default, a Cisco router will make an attempt to route almost any IP packet.
  - If a packet arrives addressed to a subnet of a network with no default network route, then IOS will use IP classless routing to forward the packet along the best available route.
- This feature is often not needed therefore on routers where IP classless routing is not needed. Disable it using the **`no ip classless`** command.

Protecting Routing Table Integrity

- Use only static routes:
  - Works well in small networks.
  - Unsuitable for large networks.
- Authenticate route table updates:
  - Configure routing authentication.
  - Authenticated router updates ensure that the update messages come from legitimate sources.

Passive Interfaces

- Configure the **`passive-interface`** command to prevent hackers from learning about the existence of certain routes or routing protocols used.

Router Hardening Considerations

- Attackers can exploit unused router services and interfaces.
- Administrators do not need to know how to exploit the services, but they should know how to disable them.
- It is tedious to disable the services individually.
- An automated method is needed to speed up the hardening process.

Locking Down Routers with AutoSecure

- The **AutoSecure** feature was released in Cisco IOS Release 12.3.
- AutoSecure is a single privileged EXEC program that allows elimination of many potential security threats quickly and easily.
  - AutoSecure helps to make you more efficient at securing Cisco routers.
- AutoSecure allows two modes of operation:
  - **Interactive mode**: Prompts to choose the way you want to configure router services and other security-related features.
  - **Noninteractive mode**: Configures security-related features on your router based on a set of Cisco defaults.

AutoSecure Can Lockdown Planes

- Management plane services and functions:
  - Finger, PAD, UDP and TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, ICMP (redirects, mask-replies), directed broadcast, MOP, banner
  - password security and SSH access
- Forwarding plane services and functions:
  - CEF, traffic filtering with ACLs
- Firewall services and functions:
  - Cisco IOS Firewall inspection for common protocols
- Login functions:
  - Password security
- NTP protocol
- SSH access
- TCP Intercept services

AutoSecure Failure Rollback Feature

- If AutoSecure fails to complete its operation, the running configuration may be corrupt:
  - In Cisco IOS Release 12.3(8)T and later releases a pre-AutoSecure configuration snapshot is stored in the flash under filename **`pre_autosec.cfg`**.
  - Rollback reverts the router to the router's pre-autosecure configuration using the **`configure replace flash:pre_autosec.cfg`** command.
  - If the router is using software prior to Cisco IOS Release 12.3(8)T, the running configuration should be saved before running AutoSecure.

AutoSecure Process Overview

- Cisco AutoSecure Interactive Steps:
  - Step 1 – Identify outside interfaces.
  - Step 2 – Secure the management plane.
  - Step 3 – Create the security banner.
  - Step 4 – Configure passwords, AAA, and SSH.
  - Step 5 – Secure the forwarding plane.

```
Router#
auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh |
firewall | tcp-intercept]
```

Auto Secure Parameters

Parameter	Description
`management`	(Optional) Only the management plane will be secured.
`forwarding`	(Optional) Only the forwarding plane will be secured.
`no-interact`	(Optional) The user will not be prompted for any interactive configurations. No interactive dialogue parameters will be configured, including usernames or passwords.
`full`	(Optional) The user will be prompted for all interactive questions. This is the default setting.
`ntp`	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command-line interface (CLI).
`login`	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
`ssh`	(Optional) Specifies the configuration of the SSH feature in the AutoSecure CLI.
`firewall`	(Optional) Specifies the configuration of the Firewall feature in the AutoSecure CLI.
`tcp-intercept`	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

Step 1: Identify Outside Interfaces

```
Router# auto secure
           --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router but it will not
make router absolutely secure from all security attacks ***
All the configuration done as part of AutoSecure will be shown here. For more
details of why and how this configuration is useful, and any possible side effects,
please refer to Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: y
Enter the number of interfaces facing internet [1]: 1
Interface     IP-Address      OK? Method Status  Protocol
Ethernet0/0   10.0.2.2        YES NVRAM  up      up
Ethernet0/1   172.30.2.2      YES NVRAM  up      up

Enter the interface name that is facing internet: Ethernet0/1
```


Step 2: Secure Management Plane

```
Securing Management plane services..
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
```


Step 3: Create Security Banner

```
Here is a sample Security Banner to be shown at every access to device. Modify it
to suit your enterprise requirements.
Authorised Access only
  This system is the property of Woolloomooloo Pty Ltd.
  UNAUTHORISED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged and violations of of this policy result
  in disciplinary action.
Enter the security banner {Put the banner between
k and k, where k is any character}:
%This system is the property of Cisco Systems, Inc.
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.%
```


Step 4: Passwords, AAA and Login Blocking

```
Enable secret is either not configured or is same as enable password
Enter the new enable secret: Cur1um96
Configuration of local user database
Enter the username: student1
Enter the password: student1
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Securing device against Login Attacks
Configure the following parameters
Blocking Period when Login Attack detected: 300
Maximum Login failures with the device: 3
Maximum time period for crossing the failed login attempts: 60
```

Step 5: SSH and Interface-Specifics

```
Configure SSH server? [yes]: y
Enter the hostname: R2
Enter the domain-name: cisco.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces
```


Step 6: Forwarding Plane and Firewall

```
Securing Forwarding plane services..
Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet
Configure CBAC Firewall feature? [yes/no]: yes
This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
.
.
Apply this configuration to running-config? [yes]: y
```


Locking Down Routers with Cisco CCP

- CCP simplifies router and security configuration through smart wizards that help to quickly and easily deploy, configure, and monitor a Cisco router without requiring knowledge of the CLI.
- CCP simplifies firewall and IOS software configuration without requiring expertise about security or IOS software.
- CCP contains a Security Audit wizard that performs a comprehensive router security audit.

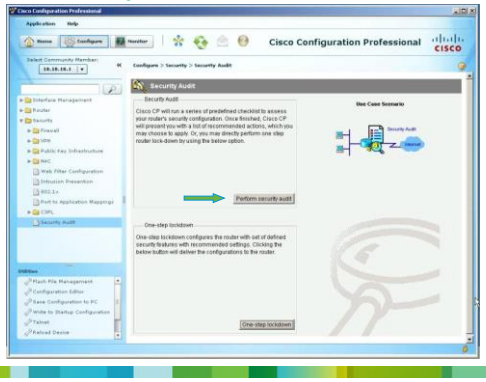
Locking Down Routers with Cisco CCP

- CCP uses security configurations recommended by Cisco Technical Assistance Center (TAC) and the International Computer Security Association (ICSA) as the basis for comparisons and default settings.
- The Security Audit wizard assesses the vulnerability of the existing router and provides quick compliance to best-practice security policies.
- CCP can implement almost all of the configurations that AutoSecure offers with the One-Step Lockdown feature.

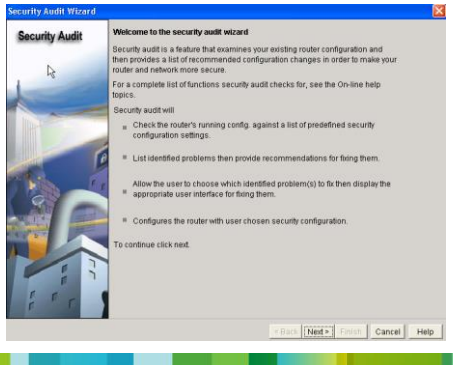
CCP Security Audit Overview

- Security Audit compares router configuration against recommended settings.
- Examples of the audit include:
  - Shut down unneeded servers.
  - Disable unneeded services.
  - Apply the firewall to the outside interfaces.
  - Disable or harden SNMP.
  - Shut down unused interfaces.
  - Check password strength.
  - Enforce the use of ACLs.

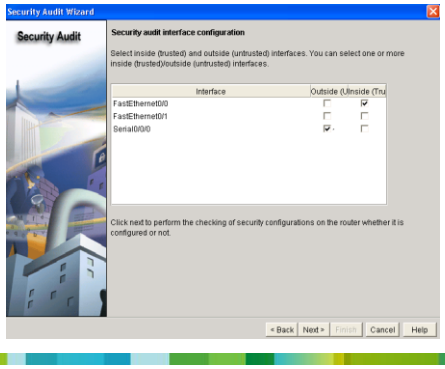
CCP Security Audit: Main Window



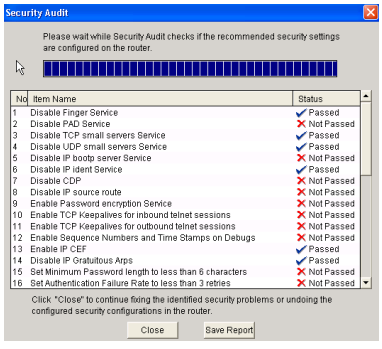
CCP Security Audit Wizard



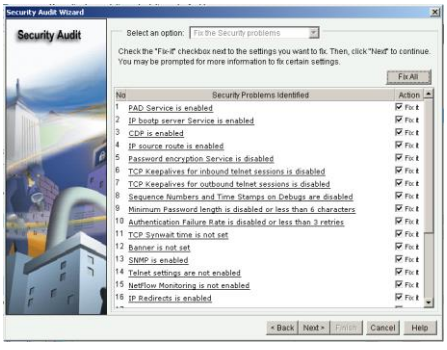
CCP Security Audit Configuration



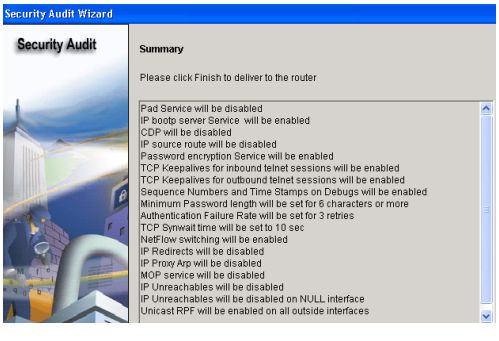
CCP Security Audit



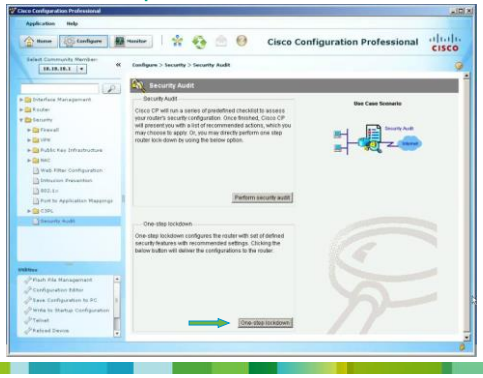
CCP Security Audit



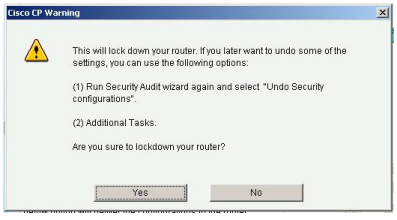
CCP Security Audit: Summary



CCP One-Step Lockdown



CCP One-Step Lockdown Wizard



Lab 2A: Securing the Router for Administrative Access

- Part 1: Basic Network Device Configuration
- Part 2: Control Administrative Access for Routers
  - Configure and encrypt all passwords.
  - Configure a login warning banner.
  - Configure enhanced username password security.
  - Configure enhanced virtual login security.
  - Configure an SSH server on a router.
  - Configure an SSH client and verify connectivity.
- Part 3: Configure Administrative Roles
  - Create multiple role views and grant varying privileges.
  - Verify and contrast views.
- Part 4: Configure Cisco IOS Resilience and Management Reporting
  - Secure the Cisco IOS image and configuration files.
  - Configure a router as a synchronized time source for other devices using NTP.
  - Configure Syslog support on a router.
  - Install a Syslog server on a PC and enable it.
  - Configure trap reporting on a router using SNMP.
  - Make changes to the router and monitor syslog results on the PC.
- Part 5: Configure Automated Security Features
  - Lock down a router using AutoSecure and verify the configuration.
  - Use the CCP Security Audit tool to identify vulnerabilities and to lock down services.
  - Contrast the AutoSecure configuration with CCP.