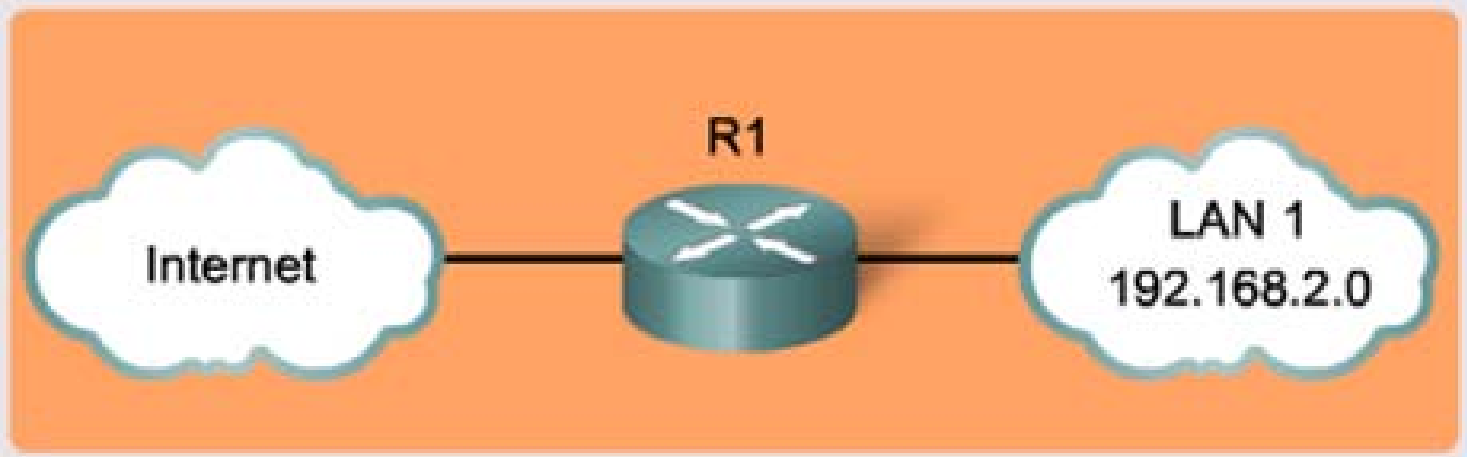
Network Security

- Secure the physical installation of and the administrative access to Cisco routers based on different network requirements using the CLI and SDM.
- Configure administrative roles using privilege levels and role-based CLI.
- Implement the management and reporting features of syslog, SNMP, SSH, and NTP.
- Examine router configurations with the Security Audit feature of Cisco SDM, and make the router and network more secure by using the auto secure command or the One-Step Lockdown feature of Cisco SDM.

Network Security

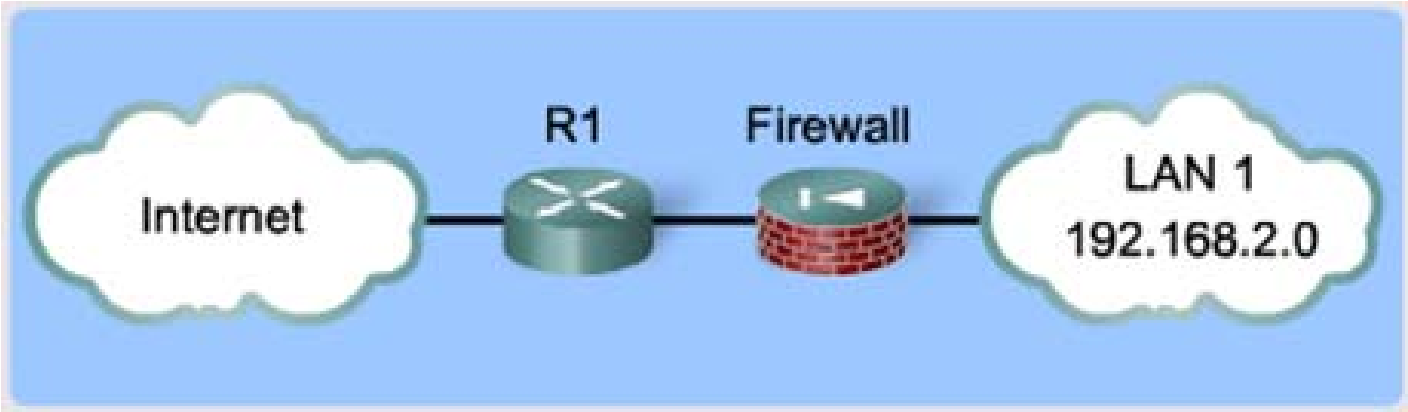
- Routers are used to secure the perimeter of networks.
  - Single router approach



Network Security

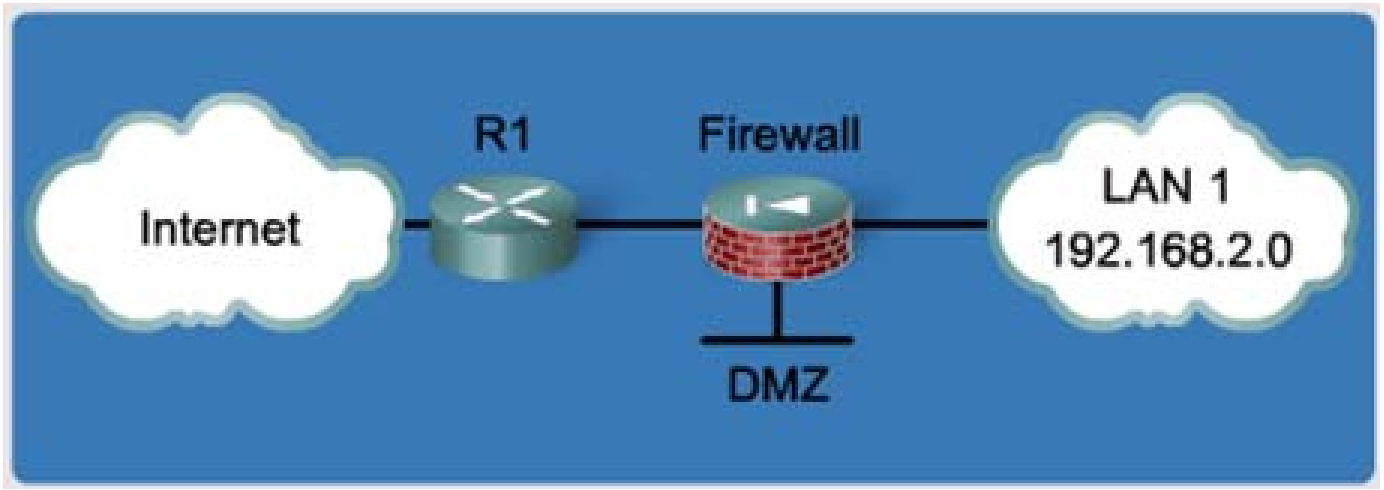
Cisco.com

- Defence-in-depth approach
  - A router screening traffic before a dedicated firewall appliance(e.g. ASA)



Network Security

- DMZ approach
  - DMZ containing servers that must be accessed from the untrusted outside



Physical Security

- Secure locked room
- Free of electrostatic or magnetic interference
- Fire suppression
- Temperature and humidity
- UPS

Operating system security

- Features and performance
- Maximum amount of memory possible
- Latest stable version
- Secure copy
  - Router operating system image
  - Router configuration file

Router hardening

Cisco.com

- Secure administrative control
  - Restrict device accessibility
  - Log and account for all access
  - Authenticate access
  - Authorize actions
  - Present legal notification
  - Ensure the confidentiality of data
- Disable unused ports and interfaces
- Disable unnecessary services.

Secure passwords

- Use a password length of 10 or more characters.
- Make passwords complex. Include 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.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

Passwords - con 0

Cisco.com

```
R1(config)# service password-encryption
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>
```

Passwords – vty 0 4

Cisco.com

```
R1# configure terminal
R1(config)# username ADMIN secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# exit
R1(config)# login block-for 15 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
```

Banners

Cisco.com

- Present legal notification
  - banner {exec | incoming | login | motd | slip-ppp} d message d

Configure SSH

Step 1: Configure the IP domain name

Step 2: Generate one-way secret keys

Step 3: Verify or create a local database entry

Step 4: Enable VTY inbound SSH sessions

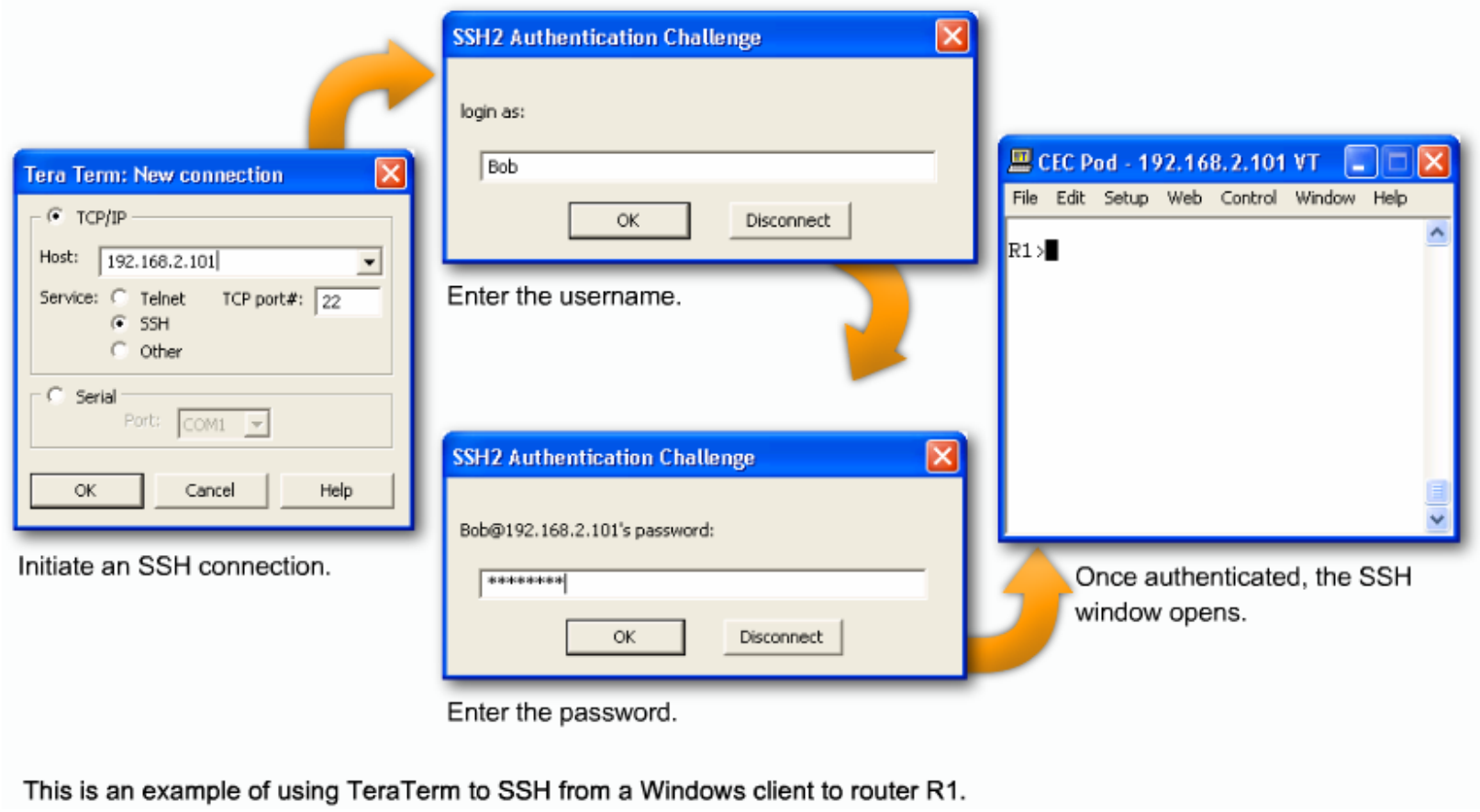
Configure SSH


```
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
```

Configure SSH


```
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 time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 2
R1#
```

Configure SSH



This is an example of using TeraTerm to SSH from a Windows client to router R1.

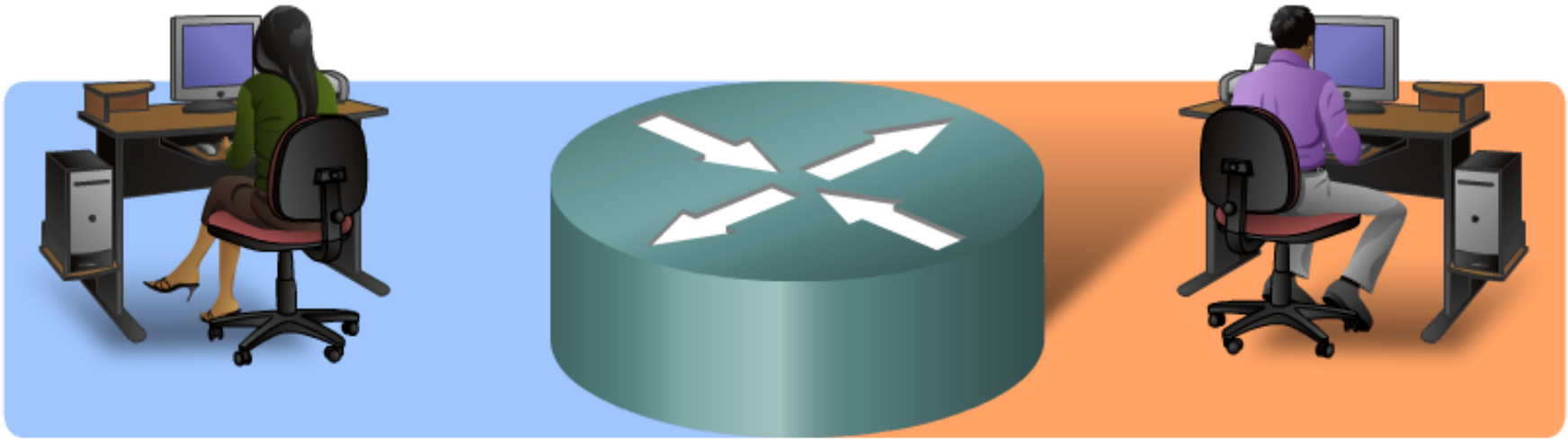
Privilege levels

Security Operator Privileges

- Configure AAA
- Issue **show** Commands
- Configure Firewall
- Configure IDS/IPS
- Configure NetFlow

WAN Engineer Privileges

- Configure Routing
- Configure Interfaces
- Issue **show** Commands



Privilege levels

- Level 0: Predefined for user-level access privileges. Seldom used, but includes five commands: disable, enable, exit, help, and logout
- Level 1: 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 another higher level, or commands from higher levels may be moved down to a lower level.
- Level 15: Reserved for the enable mode privileges (enable command). Users can change configurations and view configuration files.

Privilege levels

Cisco.com

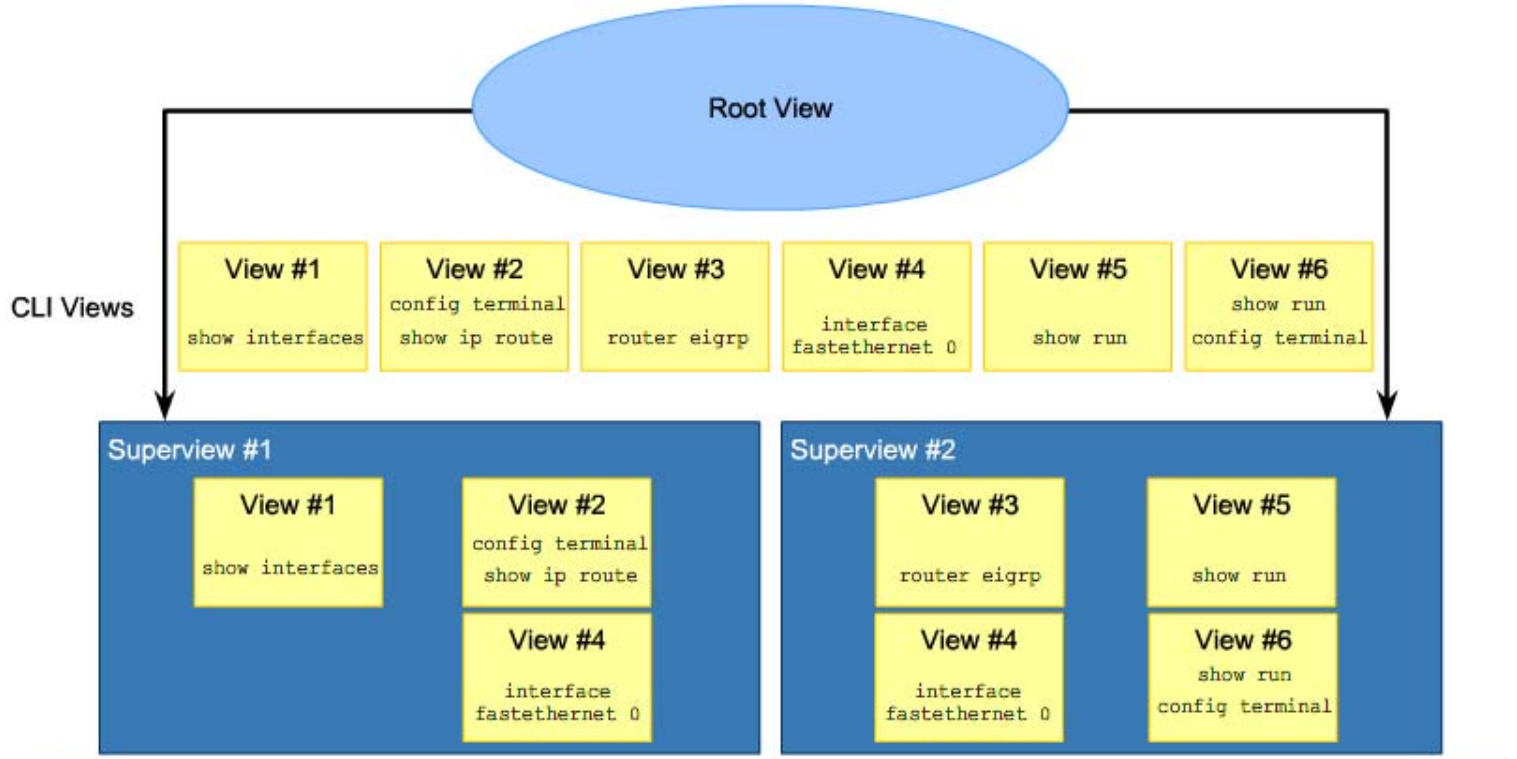
```
R1# conf t
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level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

Role Based CLI access

- The biggest limitation however is that 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.

- How can the limitations of assigning privilege levels be overcome?

Role Based CLI Access



Superviews contain Views but not commands. Two Superviews can use the same View. For example, both superview 1 and superview 2 can have CLI view 4 placed inside.

Role Based CLI Access

- Step 1. Enable AAA with the aaa new-model global configuration command. Exit and enter the root view with the enable view command.
- Step 2. Create a view using the parser view view-name command. This enables the view configuration mode. Excluding the root view, there is a maximum limit of 15 views in total.
- Step 3. Assign a secret password to the view using the secret encrypted-password command.
- Step 4. Assign commands to the selected view using the commands parser-mode {include | include-exclusive | exclude} [all] [interface interface-name | command] command in view configuration mode.
- Step 5. Exit view configuration mode by typing the exit command.

Role Based CLI Access


```
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
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
R1(config)#
```

Role Based CLI Access


```
R1(config-view)#exit
R1(config)#
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
R1(config)#
```

Cisco IOS Resilient Configuration

- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.

Cisco IOS Resilient Configuration

- Step 1. Reload the router using the reload command.
- Step 2. From ROMmon mode, enter the dir command to list the contents of the device that contains the secure bootset file. From the CLI, the device name can be found in the output of the show secure bootset command.
- Step 3. Boot the router with the secure bootset image using the boot command with the filename found in Step 2. When the compromised router boots, change to privileged EXEC mode and restore the configuration.
- Step 4. Enter global configuration mode using conf t.
- Step 5. Restore the secure configuration to the supplied filename using the secure boot-config restore filename command.

Recovering a router password

- Step 1. Connect to the console port.
- Step 2. Use the show version command to view and record the configuration register.
- The configuration register is similar to the BIOS setting of a computer, which controls the bootup process. A configuration register, represented by a single hexadecimal value, tells a router what specific steps to take when powered on. Configuration registers have many uses, and password recovery is probably the most used. To view and record the configuration register, use the show version command.
- R1> show version
- <Output omitted>
- Configuration register is 0x2102
- The configuration register is usually set to 0x2102 or 0x102. If there is no longer access to the router (because of a lost login or TACACS password), an administrator can safely assume that the configuration register is set to 0x2102.

Recovering a router password

- Step 3. Use the power switch to power cycle the router.
- Step 4. Issue the break sequence within 60 seconds of power up to put the router into ROMmon.
- Step 5. Type confreg 0x2142 at the rommon 1> prompt.
- This changes the default configuration register and causes the router to bypass the startup configuration where the forgotten enable password is stored.

- Step 6. Type reset at the rommon 2> prompt. The router reboots, but ignores the saved configuration.
- Step 7. Type no after each setup question, or press Ctrl-C to skip the initial setup procedure.
- Step 8. Type enable at the Router> prompt. This puts the router into enable mode and allows you to see the Router# prompt.
- Step 9. Type copy startup-config running-config to copy the NVRAM into memory. Be careful not to type copy running-config startup-config or the startup configuration will be erased.

Recovering a router password

- Step 10. Type show running-config. In this configuration, the shutdown command appears under all interfaces because all interfaces are currently shut down. An administrator can now see the passwords (enable password, enable secret, vty, and console passwords) either in encrypted or unencrypted format. Unencrypted passwords can be reused, but encrypted passwords need a new password to be created.
- Step 11. Enter global configuration and type the enable secret command to change the enable secret password. For example:
- R1(config)# enable secret cisco

Recovering a router password

- Step 12. Issue the no shutdown command on every interface to be used. Then issue the show ip interface brief command in privileged EXEC mode to confirm that the interface configuration is correct. Every interface to be used should display "up up."
- Step 13. From global configuration mode type config-register configuration_register_setting. The configuration register setting is either the value recorded in step 2 or 0x2102 . For example:
- R1(config)# config-register 0x2102
- Step 14. Save the configuration changes using the copy running-config startup-config command.

Recovering a router password

Cisco.com

```
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)
```

Syslog

- What are the most important logs?
- How are important messages separated from routine notifications?
- How do you prevent tampering with logs?
- How do you ensure the time stamps match?
- What log data is needed in criminal investigations?
- How do you deal with the volume of messages?
- How do you manage all of the devices?
- How can you track when attacks or network failures occur?

Syslog

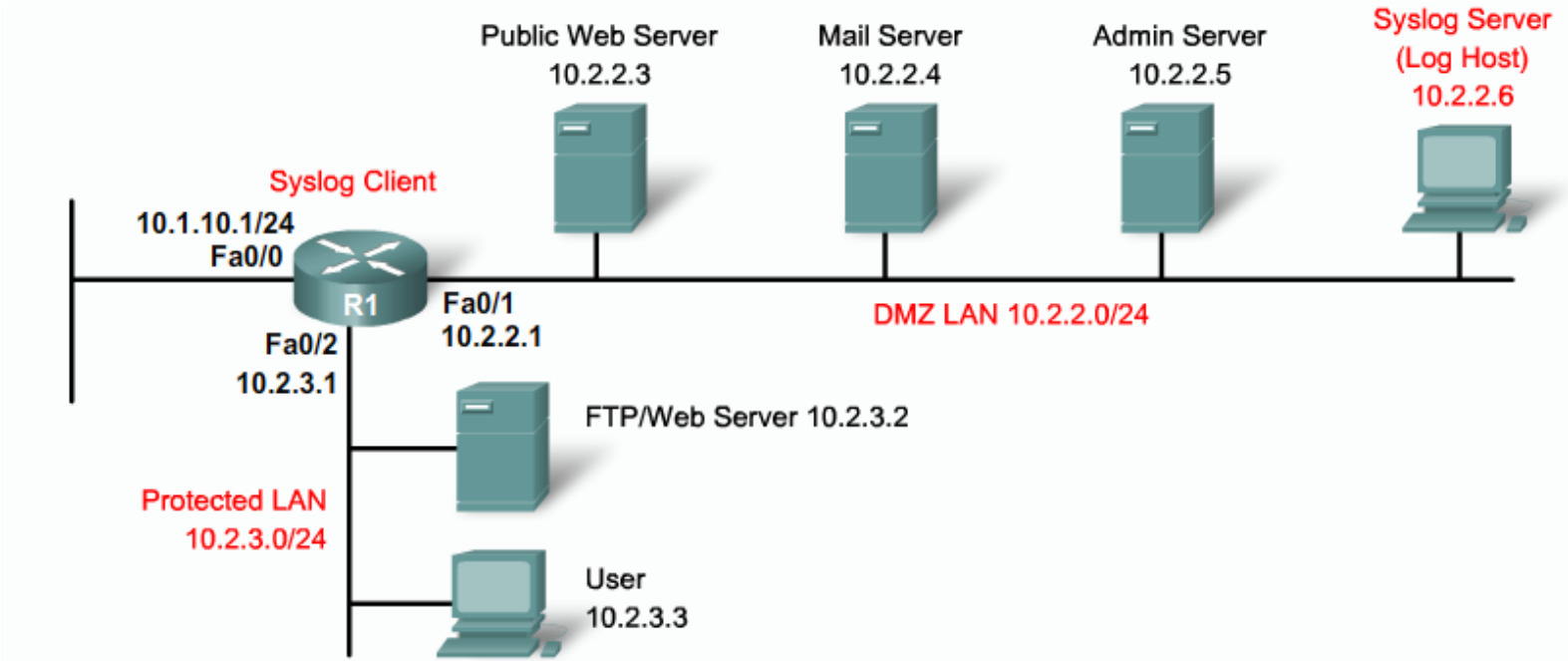
- Syslog servers - any server with the appropriate software
- Syslog clients - any router or device that generates log-messages and forwards them to the server

Syslog

- Step 1. Set the destination logging host using the logging host command.
- Step 2. (Optional) Set the log severity (trap) level using the logging trap level command.
- Step 3. Set the source interface using the logging source-interface command. This specifies that syslog packets contain the IPv4 or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.
- Step 4. Enable logging with the logging on command. You can turn logging on and off for these destinations individually using the logging buffered, logging monitor, and logging global configuration commands. However, if the logging on command is disabled, no messages are sent to these destinations. Only the console receives messages.

Syslog

Cisco.com




```
R1(config)# logging host 10.2.2.6
R1(config)# logging trap informational
R1(config)# logging source-interface loopback 0
R1(config)# logging on
```

Security Audit

Cisco.com

- Disable unnecessary services and interfaces.
- Disable and restrict commonly configured management services, such as SNMP.
- Disable probes and scans, such as ICMP.
- Ensure terminal access security.
- Disable gratuitous and proxy Address Resolution Protocol (ARP).
- Disable IP-directed broadcasts.

Security Audit

- Cisco SDM – Audit Wizard
- Cisco IOS Cli - AutoSecure

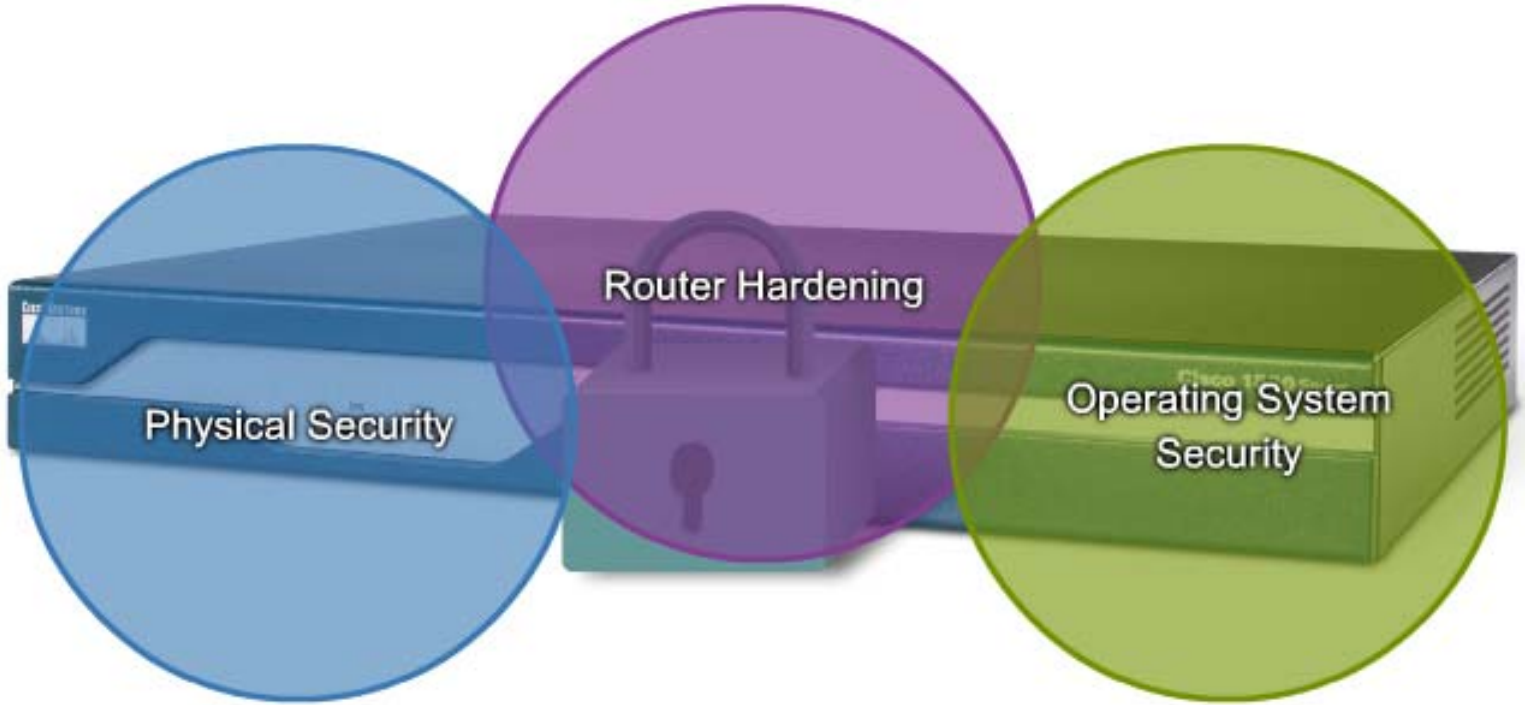
```
R1# auto secure
       --- AutoSecure Configuration ---

*** 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] :yes
```

Security Audit

Cisco.com

```
R1# auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router, but it will
not make it absolutely resistant to all security attacks ***

AutoSecure will modify the configuration of your device. All configuration
changes will be shown. For a detailed explanation of how the configuration
changes enhance security and any possible side effects, please refer to
Cisco.com for Autosecure documentation.
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

<continued>
```

Summary


Router Hardening
Physical Security
Operating System Security