CCNA Security 2.0 Study Material – Chapter 2: Securing Network Devices

itexamanswers.net/ccna-security-2-0-study-material-chapter-2-securing-network-devices.html

October 6, 2017

Chapter Outline:

Section 2.1: Securing Device Access

Upon completion of this section, you should be able to:

- Explain how to secure a network perimeter.
- Configure secure administrative access to Cisco routers.
- Configure enhanced security for virtual logins.
- Configure an SSH daemon for secure remote management.

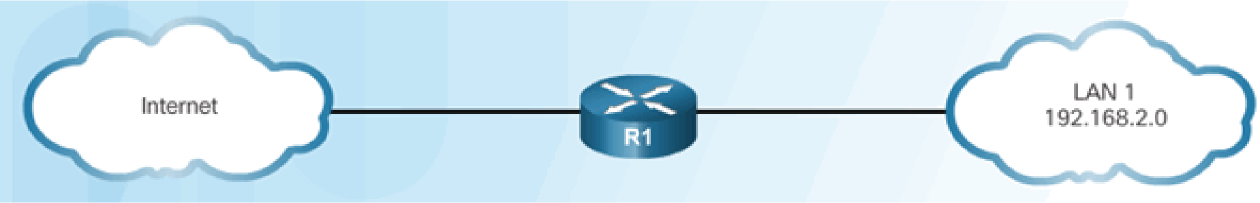
Topic 2.1.1: Securing the Edge Router

Securing the Network Infrastructure

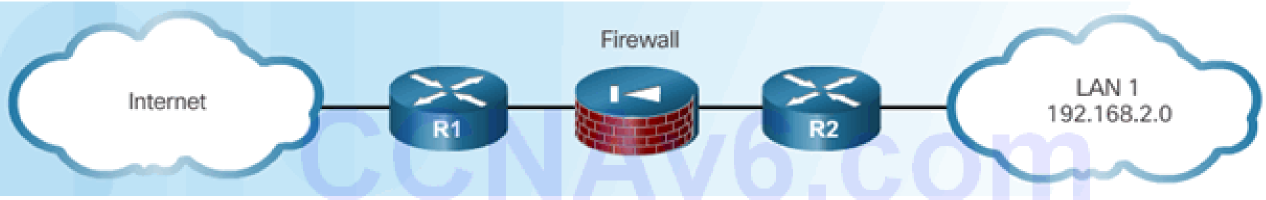
```
R1#erase startup-config
R1#reload in 5
Proceed with reload?
[confirm]
R1#
***
*** -- SHUTDOWN in 0:05:00 --
***
R1#
```

Edge Router Security Approaches

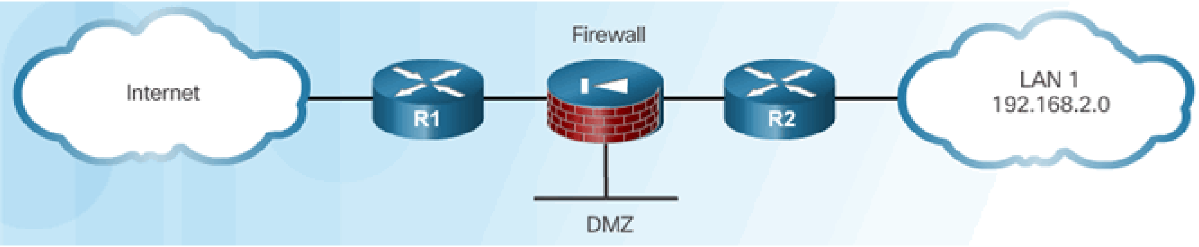
Single Router Approach



Single Router Approach



DMZ Approach



Three Areas of Router Security

Physical Security
Router Operating System and Configuration File Security
Router Hardening
Cisco 1800 Series

Secure Administrative Access

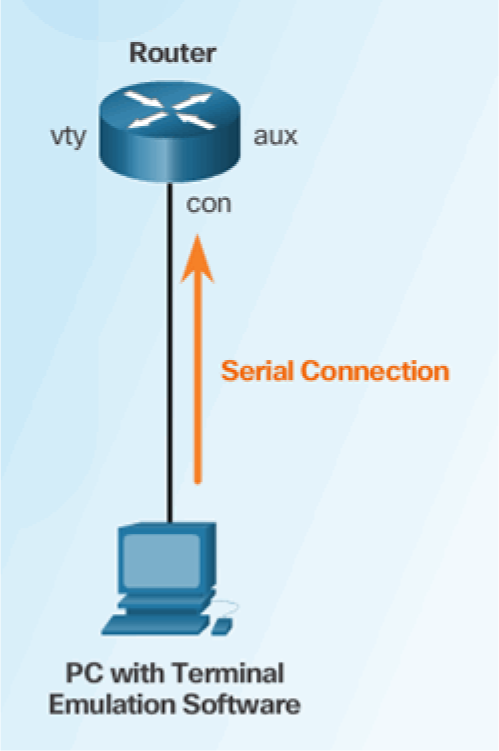
Tasks:

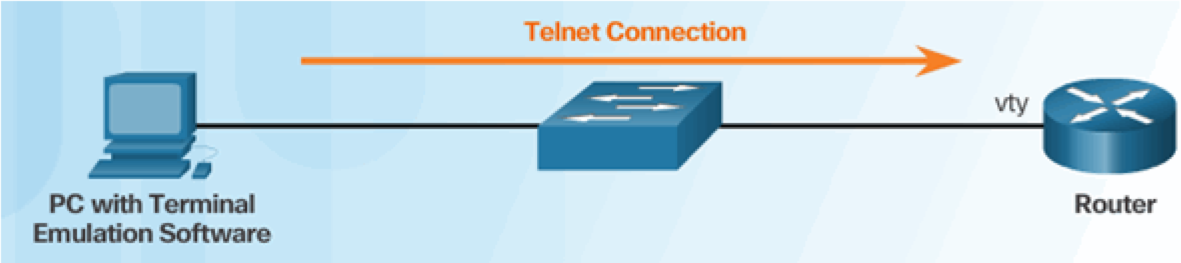
- Restrict device accessibility
- Log and account for all access
- Authenticate access
- Authorize actions
- Present legal notification
- Ensure the confidentiality of data

Secure Local and Remote Access

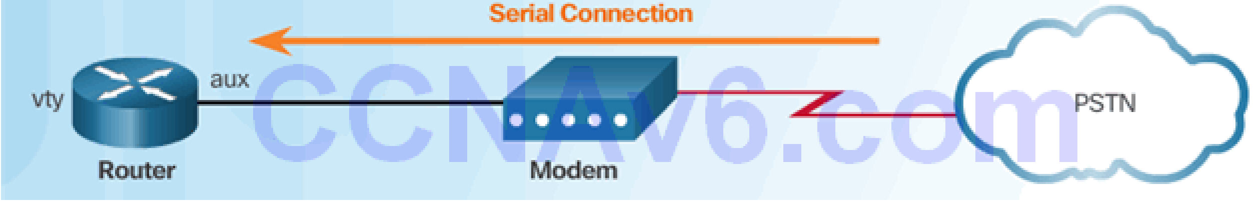
Local Access

Remote Access Using Telnet

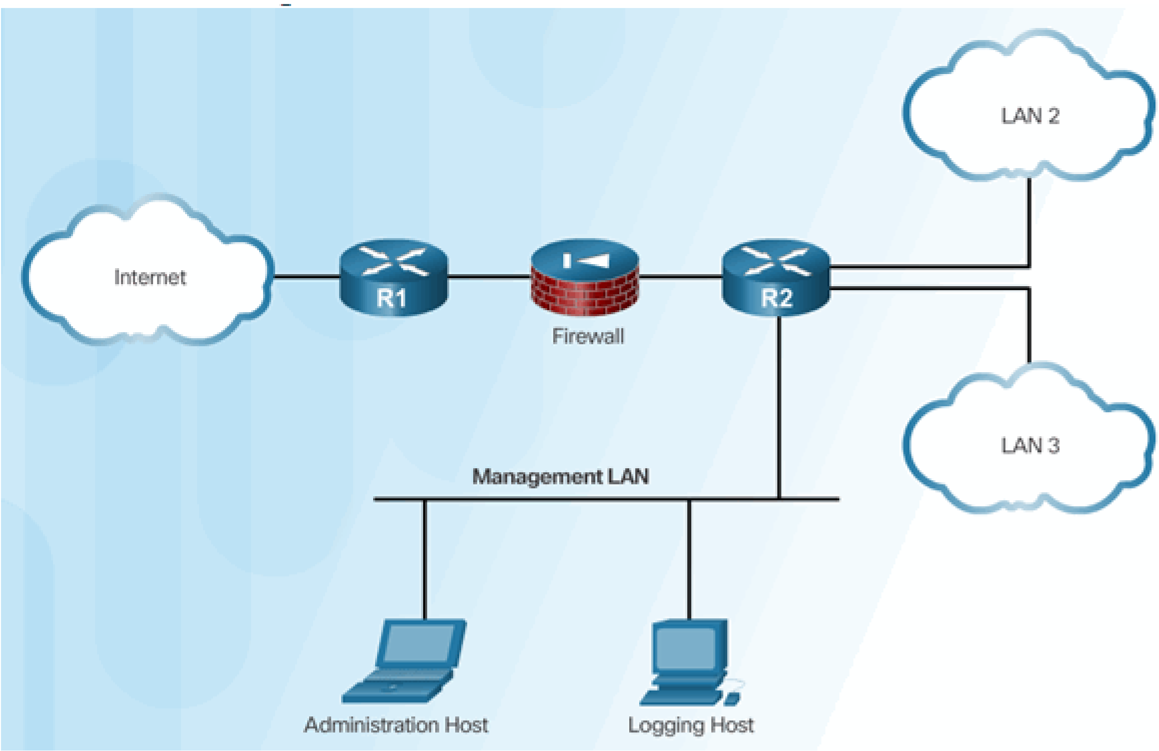




Remote Access Using Modem and Aux Port



Dedicated Management Network

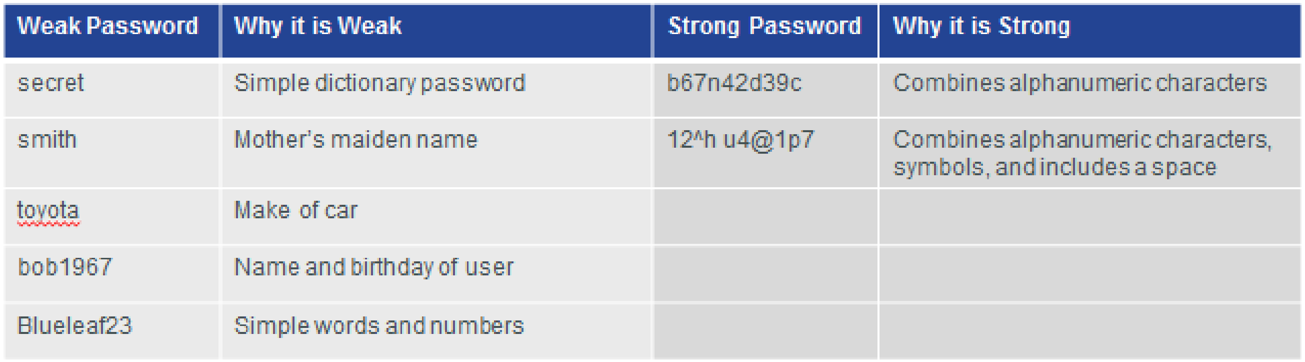


Topic 2.1.2: Configuring Secure Administrative Access

Strong Passwords

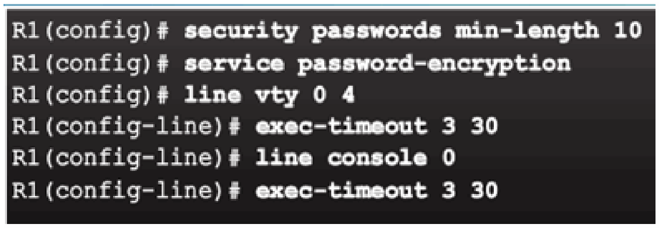
Guidelines:

- Use a password length of 10 or more characters.
- Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on easily identifiable pieces of information.
- Deliberately misspell a password (Smith = Smyth = 5mYth).
- Change passwords often.
- Do not write passwords down and leave them in obvious places.

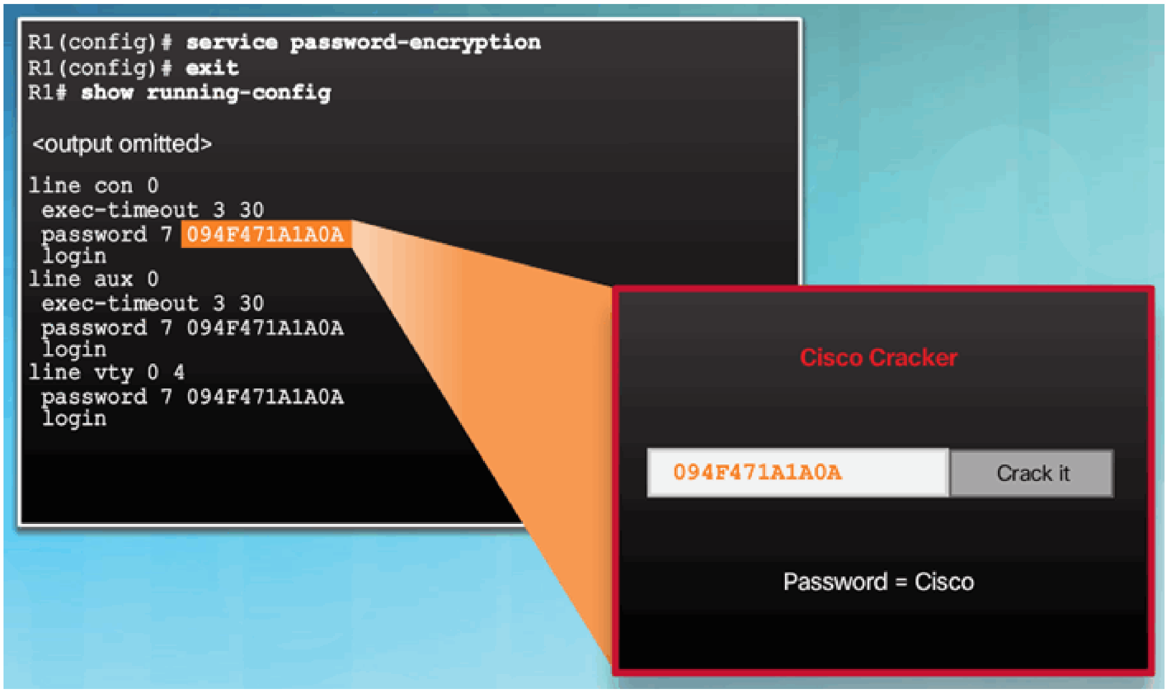


Weak Password	Why it is Weak	Strong Password	Why it is Strong
secret	Simple dictionary password	b67n42d39c	Combines alphanumeric characters
smith	Mother's maiden name	12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space
toyota	Make of car		
bob1967	Name and birthday of user		
Blueleaf23	Simple words and numbers		

Increasing Access Security



```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```



```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config

<output omitted>
line con 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line aux 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line vty 0 4
 password 7 094F471A1A0A
 login
```

Cisco Cracker

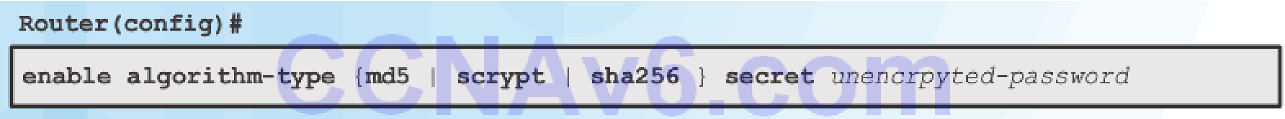
094F471A1A0A

Password = Cisco

Secret Password Algorithms

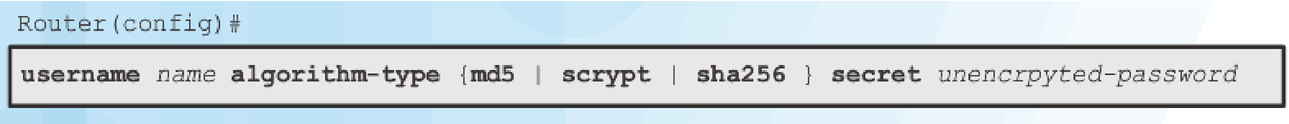
Guidelines:

- Configure all secret passwords using type 8 or type 9 passwords
- Use the enable algorithm-type command syntax to enter an unencrypted password



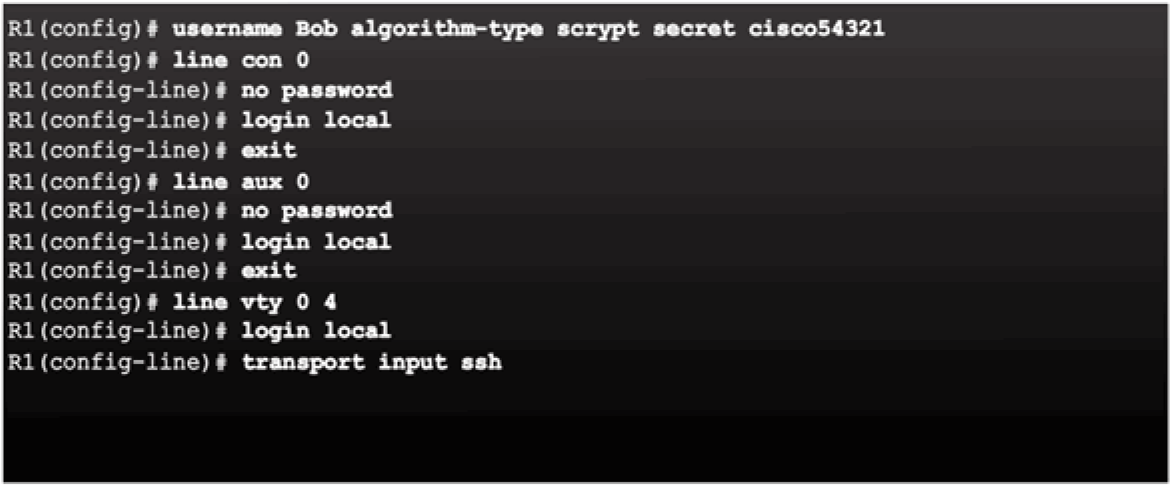
```
Router(config)#
enable algorithm-type {md5 | scrypt | sha256 } secret unencrpyted-password
```

Use the username name algorithm-type command to specify type 9 encryption



```
Router(config)#
username name algorithm-type {md5 | scrypt | sha256 } secret unencrpyted-password
```

Securing Line Access



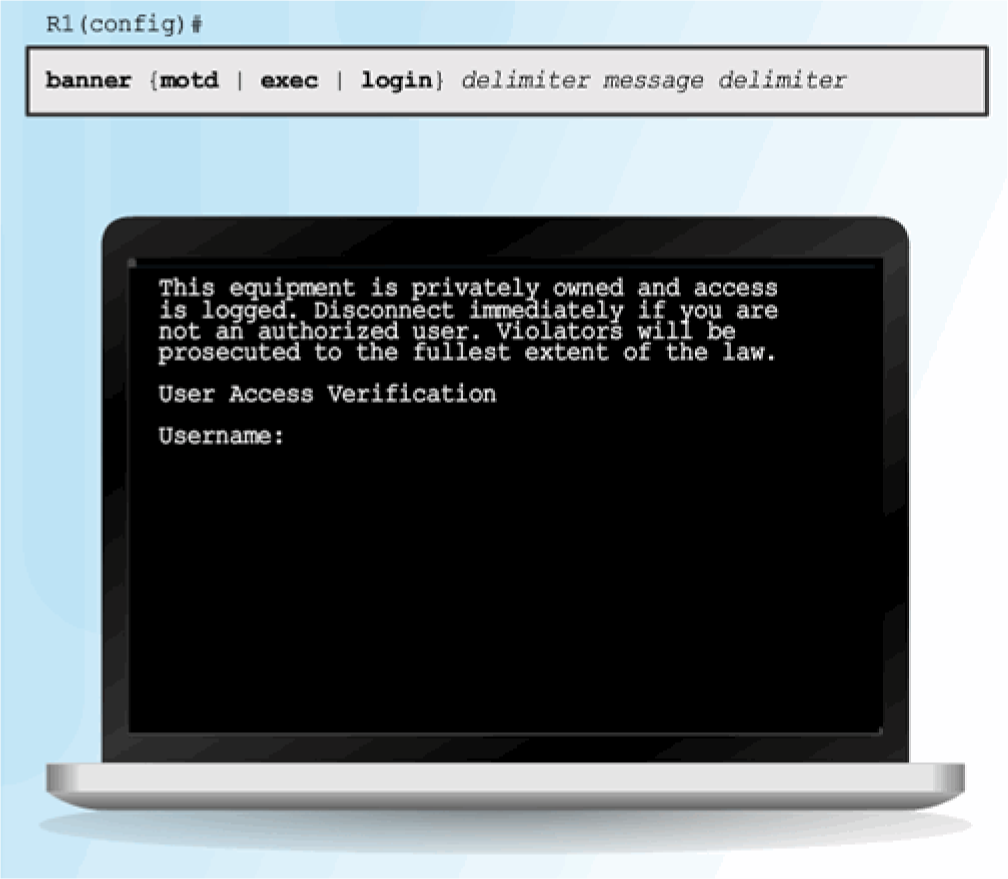
```
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line con 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

Topic 2.1.3: Configuring Enhanced Security for Virtual Logins

Enhancing the Login Process

Virtual login security enhancements:

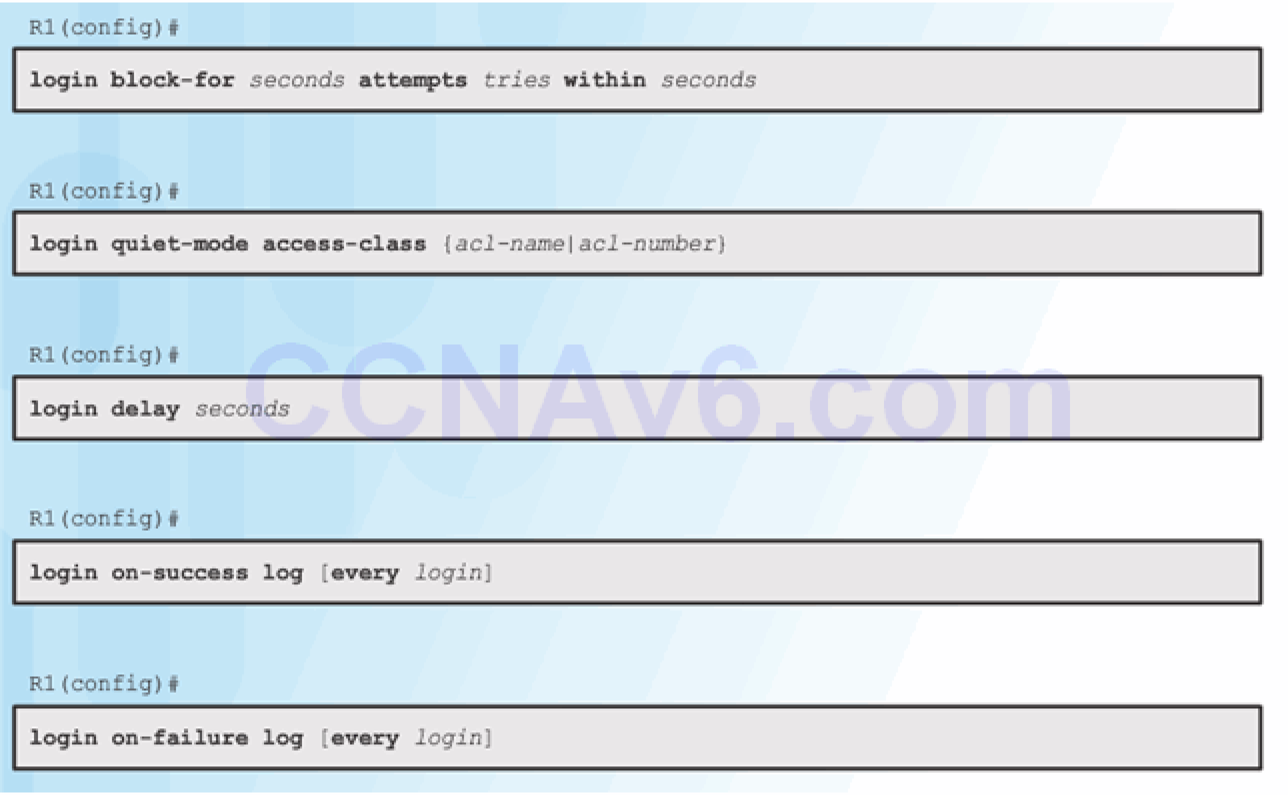
- Implement delays between successive login attempts
- Enable login shutdown if DoS attacks are suspected
- Generate system-logging messages for login detection



```
R1(config)#
banner {motd | exec | login} delimiter message delimiter
```

```
This equipment is privately owned and access
is logged. Disconnect immediately if you are
not an authorized user. Violators will be
prosecuted to the fullest extent of the law.

User Access Verification

Username:
```

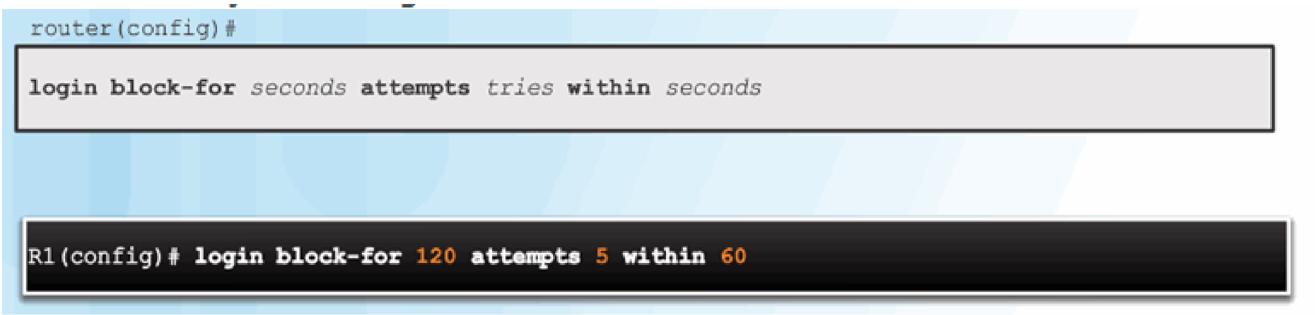
Configuring Login Enhancement Features



```
R1(config)#
login block-for seconds attempts tries within seconds

R1(config)#
login quiet-mode access-class {acl-name|acl-number}

R1(config)#
login delay seconds

R1(config)#
login on-success log [every login]

R1(config)#
login on-failure log [every login]
```

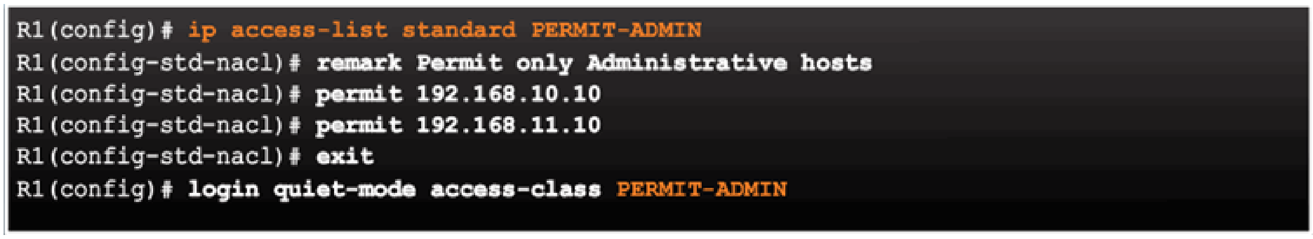
Enable Login Enhancements

Command Syntax: **login block-for**



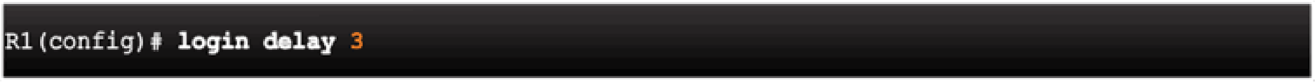
```
router(config)#
login block-for seconds attempts tries within seconds

R1(config)# login block-for 120 attempts 5 within 60
```

Example: **login quiet-mode access-class**



```
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
```

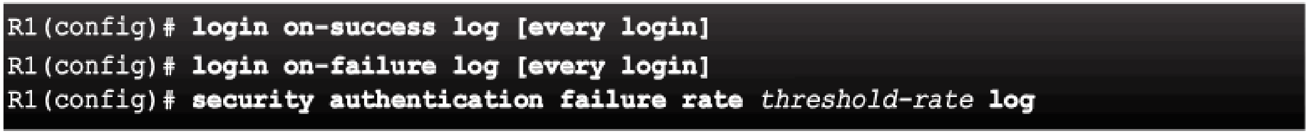
Example: **login delay**



```
R1(config)# login delay 3
```

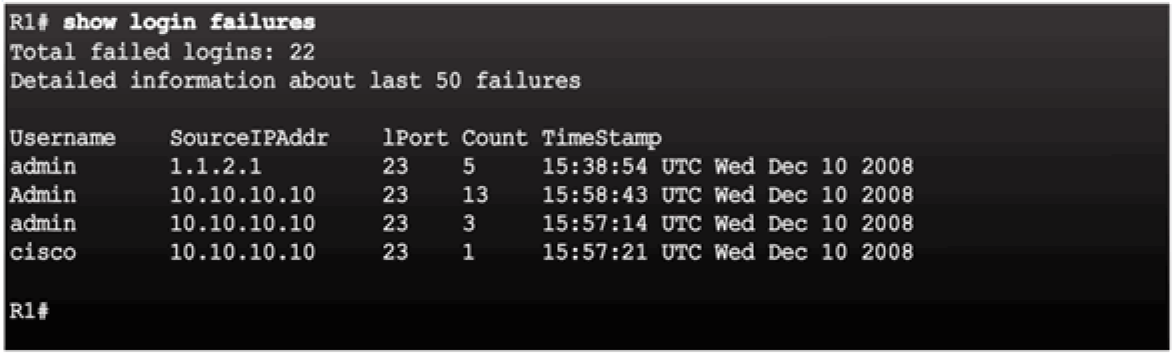
Logging Failed Attempts

Generate Login Syslog Messages



```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# security authentication failure rate threshold-rate log
```

Example: **show login failures**

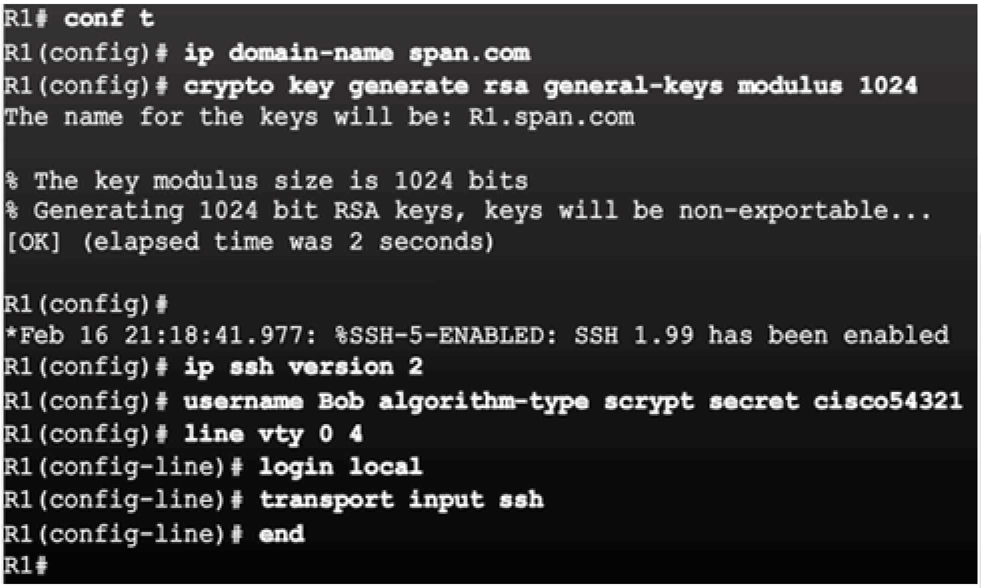


```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username    SourceIPAddr    lPort Count TimeStamp
admin       1.1.2.1         23    5     15:38:54 UTC Wed Dec 10 2008
Admin       10.10.10.10     23    13    15:58:43 UTC Wed Dec 10 2008
admin       10.10.10.10     23    3     15:57:14 UTC Wed Dec 10 2008
cisco       10.10.10.10     23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

Topic 2.1.4: Configuring SSH

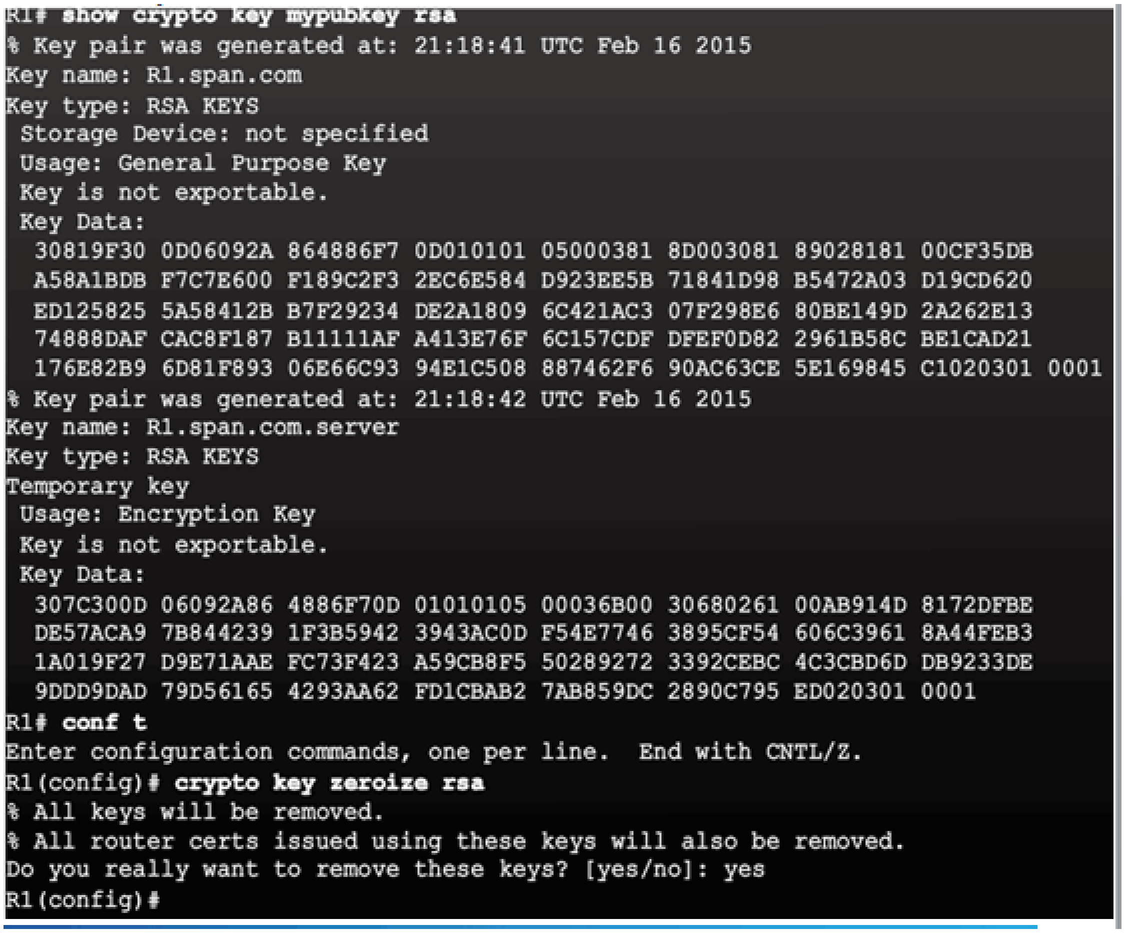
Steps for Configuring SSH

Example SSH Configuration



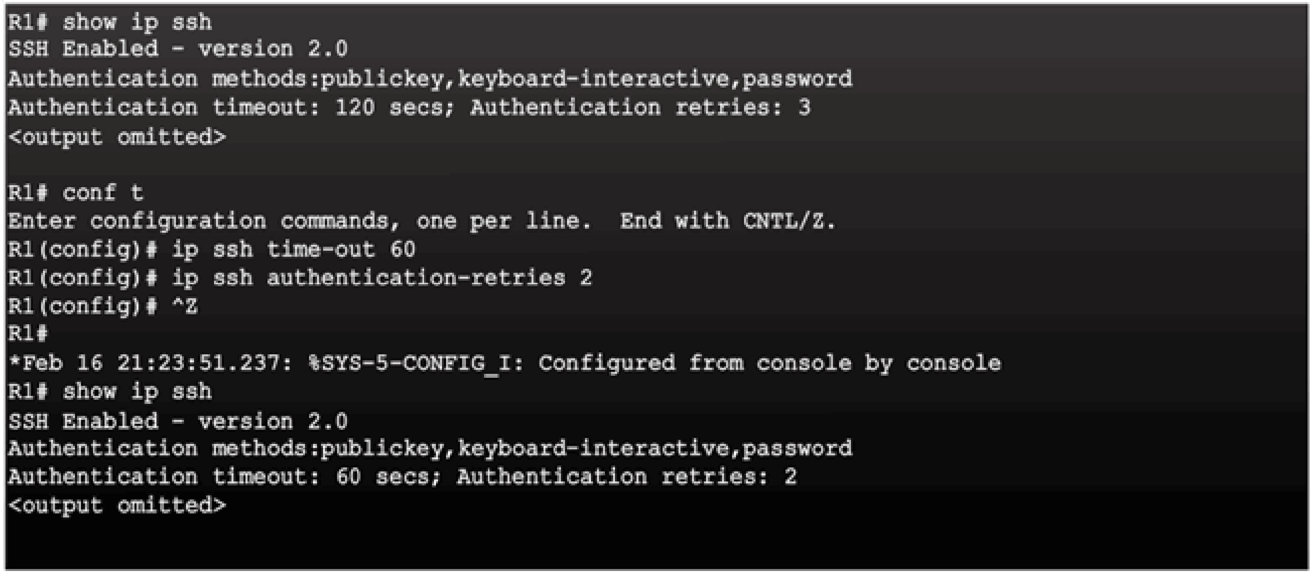
```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Feb 16 21:18:41.977: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# ip ssh version 2
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
```

Example Verification of SSH



```
R1# show crypto key mypubkey rsa
% Key pair was generated at: 21:18:41 UTC Feb 16 2015
Key name: R1.span.com
Key type: RSA KEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF35DB
  A58A1BDB F7C7E600 F189C2F3 2EC6E584 D923EE5B 71841D98 B5472A03 D19CD620
  ED125825 5A58412B B7F29234 DE2A1809 6C421AC3 07F298E6 80BE149D 2A262E13
  74888DAF CAC8F187 B11111AF A413E76F 6C157CDF DFEF0D82 2961B58C BE1CAD21
  176E82B9 6D81F893 06E66C93 94E1C508 887462F6 90AC63CE 5E169845 C1020301 0001
% Key pair was generated at: 21:18:42 UTC Feb 16 2015
Key name: R1.span.com.server
Key type: RSA KEYS
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AB914D 8172DFBE
  DE57ACA9 7B844239 1F3B5942 3943AC0D F54E7746 3895CF54 606C3961 8A44FEB3
  1A019F27 D9E71AAE FC73F423 A59CB8F5 50289272 3392CEBC 4C3CBD6D DB9233DE
  9DDD9DAD 79D56165 4293AA62 FD1CBAB2 7AB859DC 2890C795 ED020301 0001
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# crypto key zeroize rsa
% All keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R1(config)#
```

Modifying the SSH Configuration



```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
<output omitted>

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
*Feb 16 21:23:51.237: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
<output omitted>
```

Connecting to an SSH-Enabled Router

Two ways to connect:

- Enable SSH and use a Cisco router as an SSH server or SSH client.
    - As a server, the router can accept SSH client connections
    - As a client, the router can connect via SSH to another SSH-enabled router
- Use an SSH client running on a host, such as PuTTY, OpenSSH, or TeraTerm.

Section 2.2: Assigning Administrative Roles

Upon completion of this section, you should be able to:

- Configure administrative privilege levels to control command availability.
- Configure role-based CLI access to control command availability.

Topic 2.2.1: Configuring Privilege Levels

Limiting Command Availability

Privilege levels:

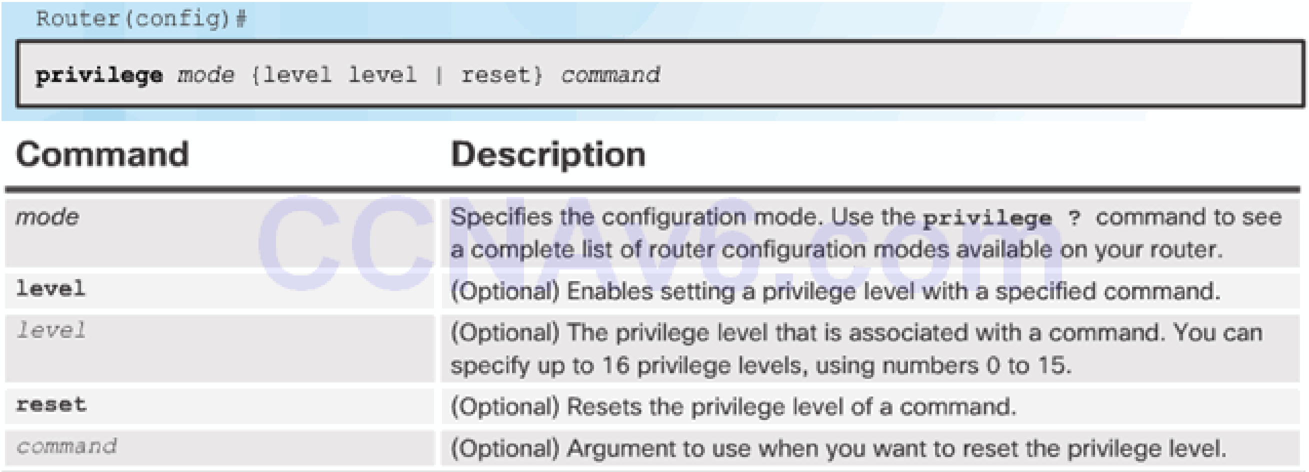
- Level 0: Predefined for user-level access privileges.
- Level 1: Default level for login with the router prompt.
- Level 2-14: May be customized for user-level privileges.
- Level 15: Reserved for the enable mode privileges.

Levels of access commands:

- User EXEC mode (privilege level 1)
    - Lowest EXEC mode user privileges
    - Only user-level command available at the router> prompt
- Privileged EXEC mode (privilege level 15)

    All enable-level commands at the router# prompt

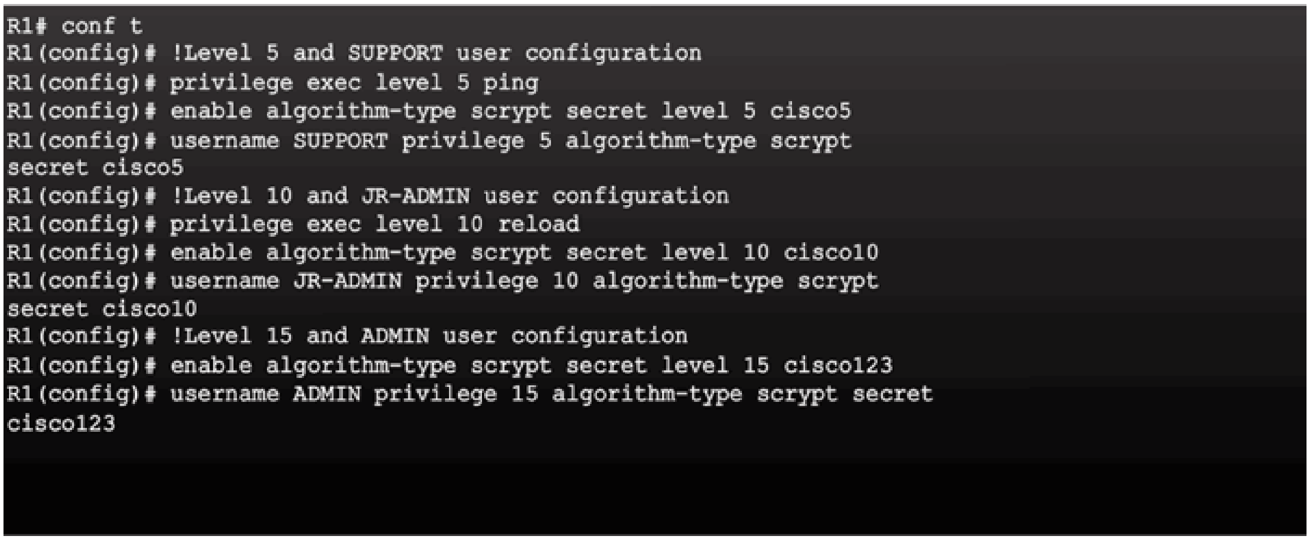
Privilege Level Syntax



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

Command	Description
mode	Specifies the configuration mode. Use the **privilege ?** command to see a complete list of router configuration modes available on your router.
level	(Optional) Enables setting a privilege level with a specified command.
level	(Optional) The privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) Resets the privilege level of a command.
command	(Optional) Argument to use when you want to reset the privilege level.

Configuring and Assigning Privilege Levels



```
R1# conf t
R1(config)# !Level 5 and SUPPORT user configuration
R1(config)# privilege exec level 5 ping
R1(config)# enable algorithm-type scrypt secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 algorithm-type scrypt
secret cisco5
R1(config)# !Level 10 and JR-ADMIN user configuration
R1(config)# privilege exec level 10 reload
R1(config)# enable algorithm-type scrypt secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 algorithm-type scrypt
secret cisco10
R1(config)# !Level 15 and ADMIN user configuration
R1(config)# enable algorithm-type scrypt secret level 15 cisco123
R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret
cisco123
```

Limitations of Privilege Levels

- 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 privilege levels
- Commands specifically set at higher privilege levels are not available for lower privilege users
- Assigning a command with multiple keywords allows access to all commands that use those

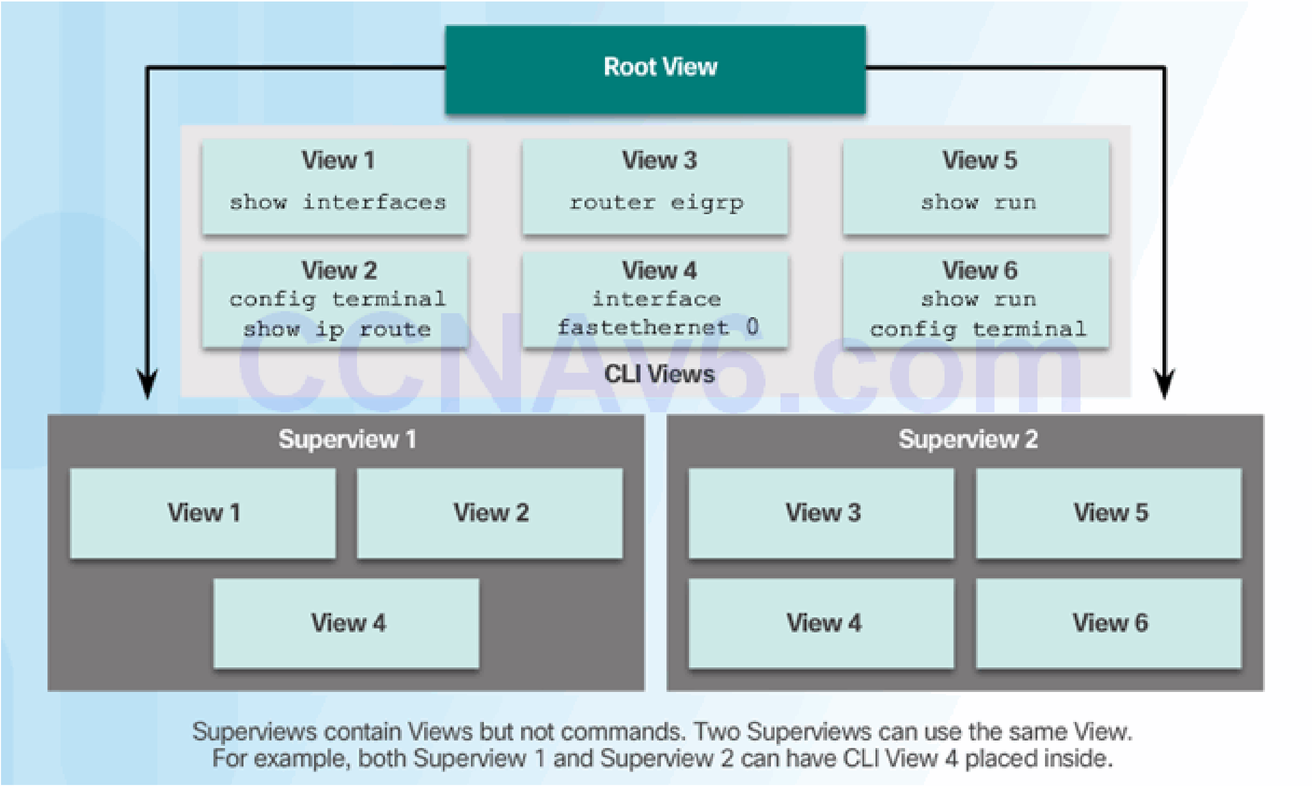
Topic 2.2.2: Configuring Role-Based CLI

Role-Based CLI Access

For example:

- 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

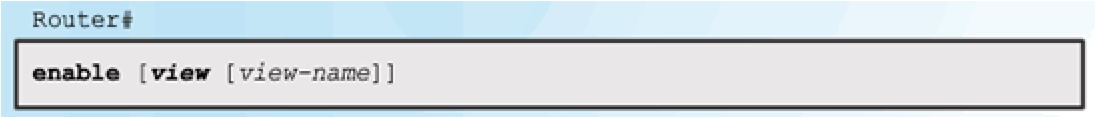
Role-Based Views



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.

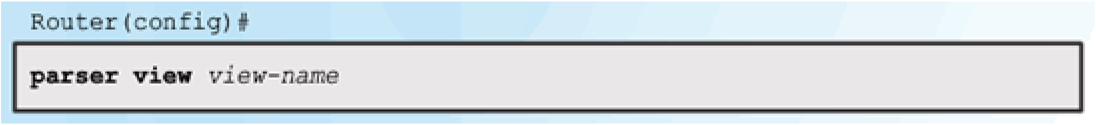
Configuring Role-Based Views

Step 1



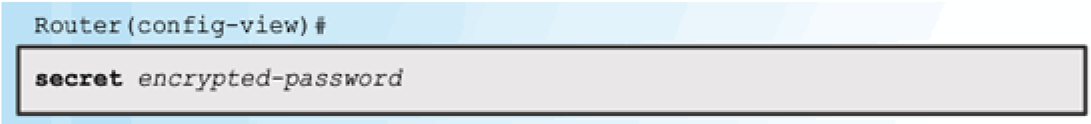
```
Router#
enable [view [view-name]]
```

Step 2



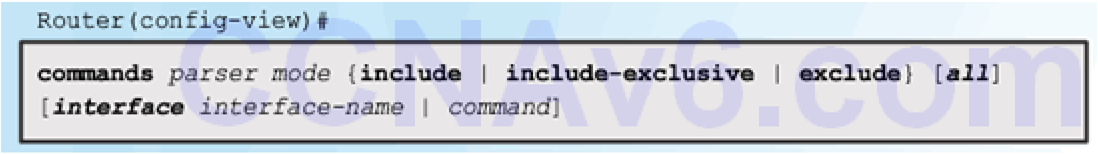
```
Router(config)#
parser view view-name
```

Step 3



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

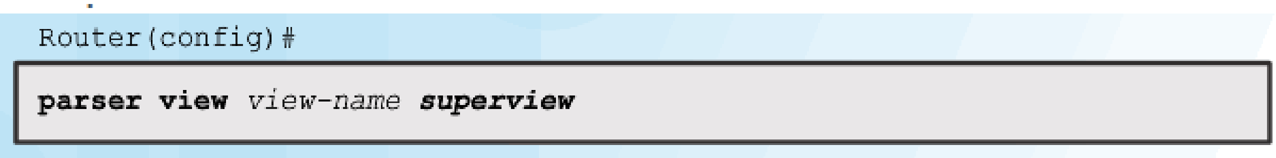
Step 4



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

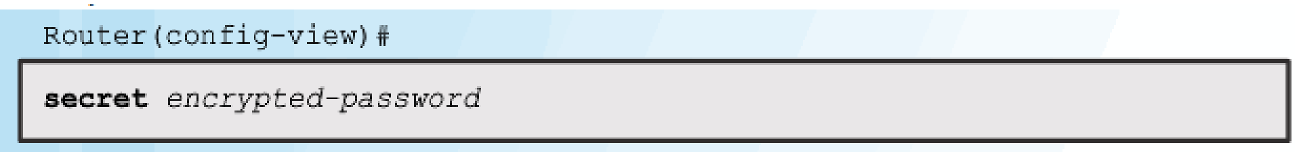
Configuring Role-Based CLI Superviews

Step 1



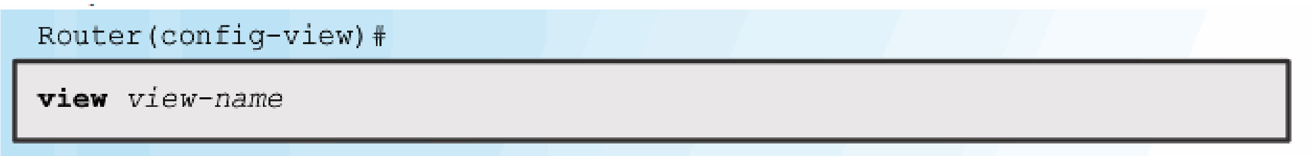
```
Router(config)#
parser view view-name superview
```

Step 2



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

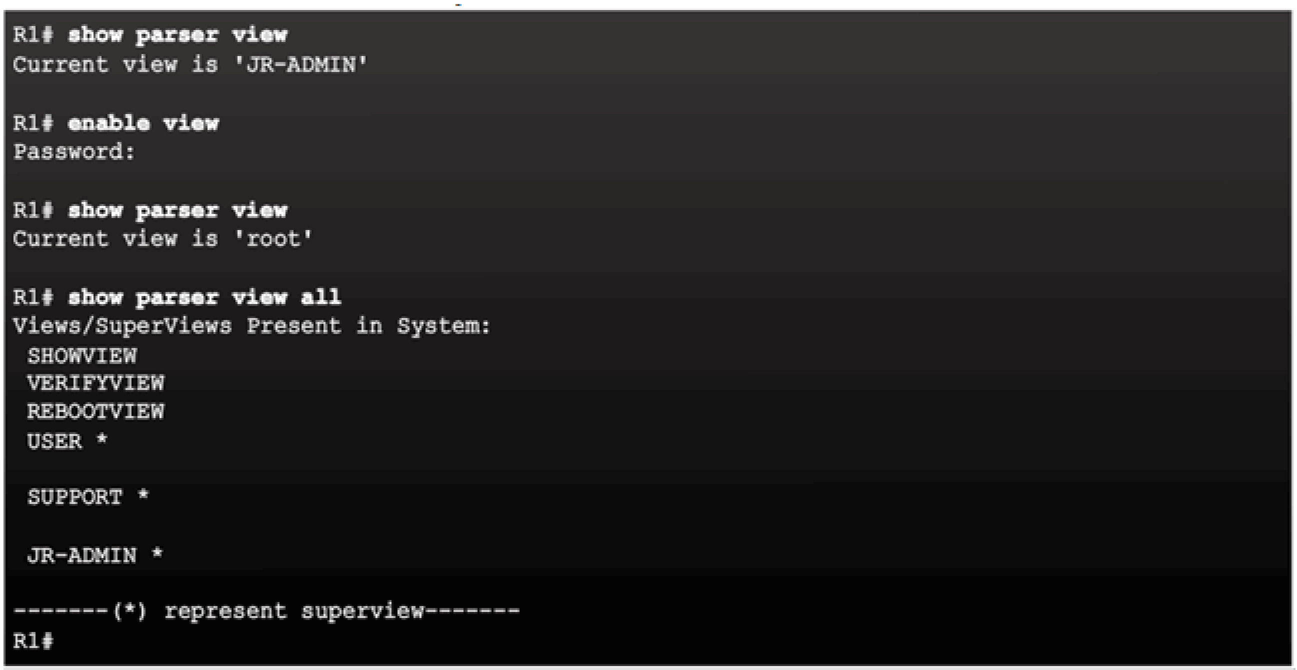
Step 3



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

Verify Role-Based CLI Views

Enable Root View and Verify All Views



```
R1# show parser view
Current view is 'JR-ADMIN'

R1# enable view
Password:

R1# show parser view
Current view is 'root'

R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 USER *

 SUPPORT *

 JR-ADMIN *

-------(*) represent superview-------
R1#
```

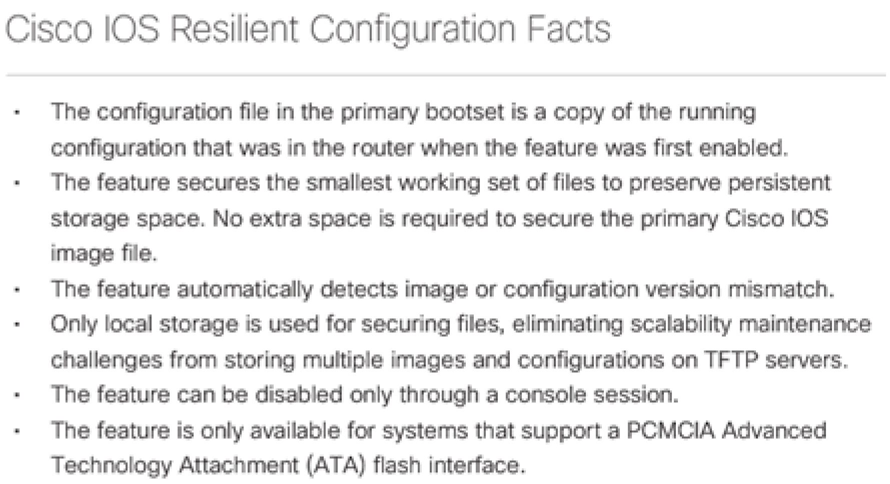
Section 2.3: Monitoring and Managing Devices

Upon completion of this section, you should be able to:

- Use the Cisco IOS resilient configuration feature to secure the Cisco IOS image and configuration files.
- Compare in-band and out-of band management access.
- Configure syslog to log system events.
- Configure secure SNMPv3 access using ACL
- Configure NTP to enable accurate timestamping between all devices.

Topic 2.3.1: Securing Cisco IOS Image and Configuration Files

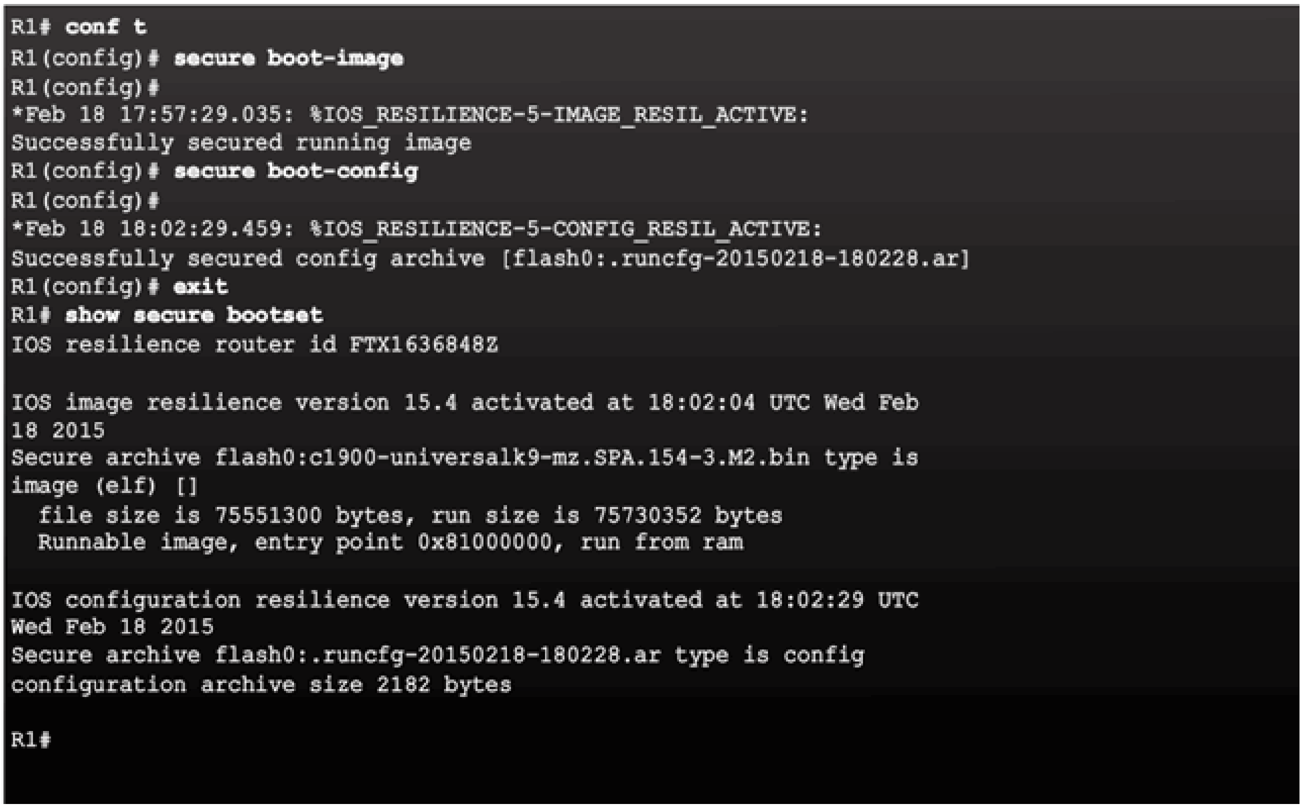
Cisco IOS Resilient Configuration Feature



Cisco IOS Resilient Configuration Facts

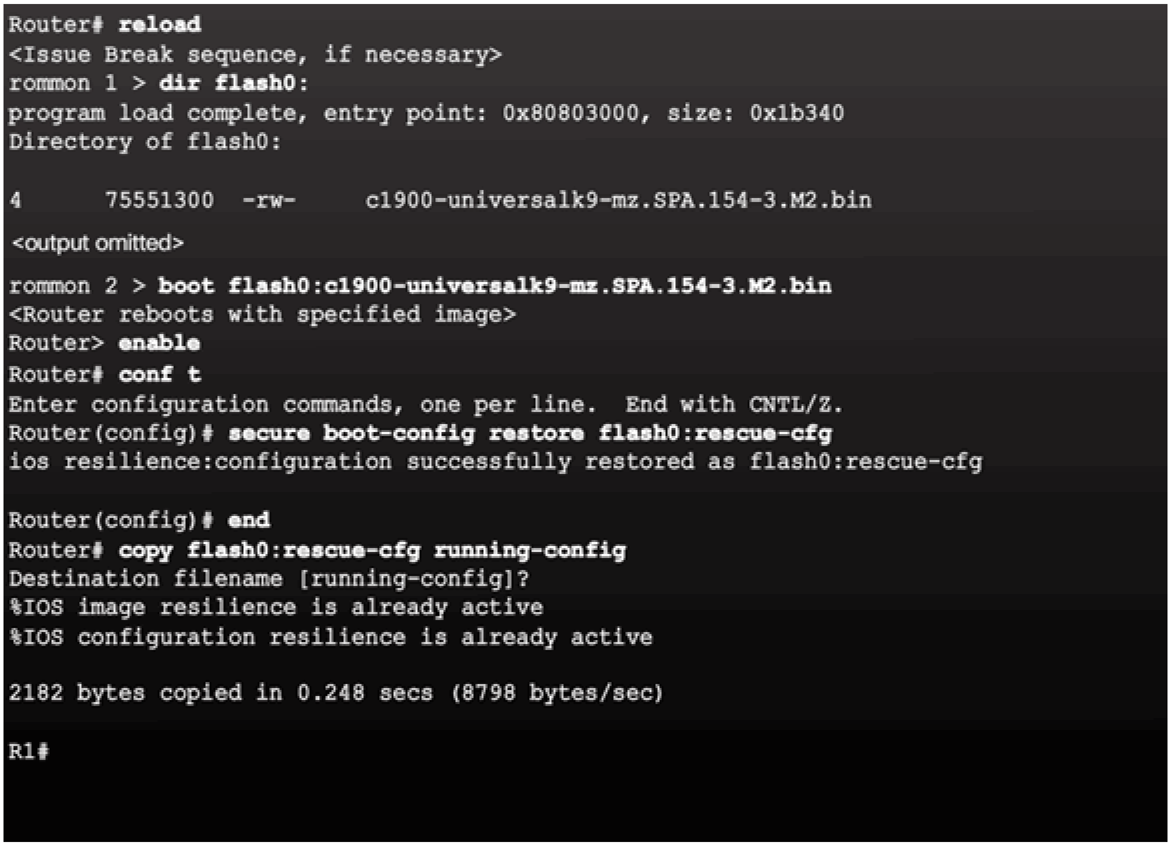
- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image 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.
- The feature is only available for systems that support a PCMCIA Advanced Technology Attachment (ATA) flash interface.

Enabling the IOS Image Resilience Feature



```
R1# conf t
R1(config)# secure boot-image
R1(config)#
*Feb 18 17:57:29.035: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE:
Successfully secured running image
R1(config)# secure boot-config
R1(config)#
*Feb 18 18:02:29.459: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE:
Successfully secured config archive [flash0:.runcfg-20150218-180228.ar]
R1(config)# exit
R1# show secure bootset
IOS resilience router id FTX1636848Z

IOS image resilience version 15.4 activated at 18:02:04 UTC Wed Feb
18 2015
Secure archive flash0:c1900-universalk9-mz.SPA.154-3.M2.bin type is
image (elf) []
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x81000000, run from ram

IOS configuration resilience version 15.4 activated at 18:02:29 UTC
Wed Feb 18 2015
Secure archive flash0:.runcfg-20150218-180228.ar type is config
configuration archive size 2182 bytes

R1#
```

The Primary Bootset Image



```
Router# reload
<Issue Break sequence, if necessary>
rommon 1 > dir flash0:
program load complete, entry point: 0x80803000, size: 0x1b340
Directory of flash0:

4      75551300  -rw-     c1900-universalk9-mz.SPA.154-3.M2.bin
<output omitted>
rommon 2 > boot flash0:c1900-universalk9-mz.SPA.154-3.M2.bin
<Router reboots with specified image>
Router> enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# secure boot-config restore flash0:rescue-cfg
ios resilience:configuration successfully restored as flash0:rescue-cfg

Router(config)# end
Router# copy flash0:rescue-cfg running-config
Destination filename [running-config]?
%IOS image resilience is already active
%IOS configuration resilience is already active

2182 bytes copied in 0.248 secs (8798 bytes/sec)

R1#
```

Configuring Secure Copy

Configure the router for server-side SCP with local AAA:

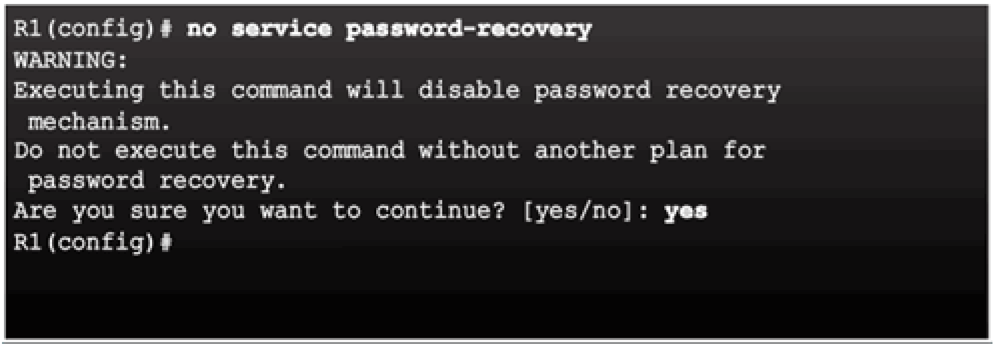
1. Configure SSH
2. Configure at least one user with privilege level 15
3. Enable AAA
4. Specify that the local database is to be used for authentication
5. Configure command authorization
6. Enable SCP server-side functionality

Recovering a Router Password

1. Connect to the console port.
2. Record the configuration register setting.
3. Power cycle the router.
4. Issue the break sequence.
5. Change the default configuration register with the confreg 0x2142 command.
6. Reboot the router.
7. Press Ctrl-C to skip the initial setup procedure.
8. Put the router into privileged EXEC mode.
9. Copy the startup configuration to the running configuration.
10. Verify the configuration.
11. Change the enable secret password.
12. Enable all interfaces.
13. Change the config-register with the config-register configuration_register_setting.
14. Save the configuration changes.

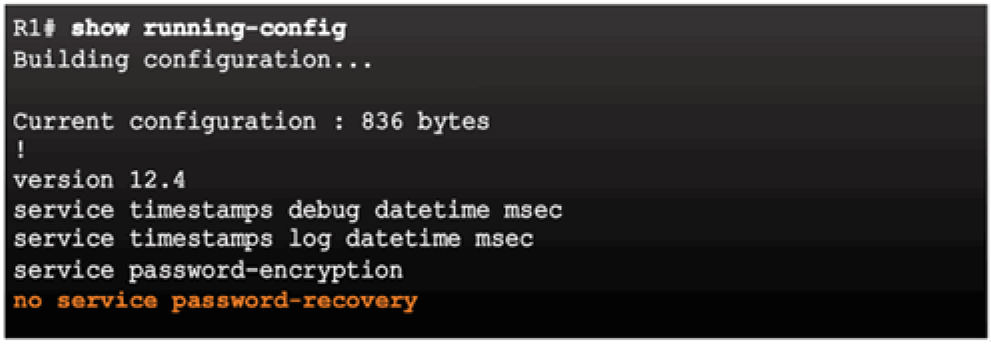
Password Recovery

Disable Password Recovery



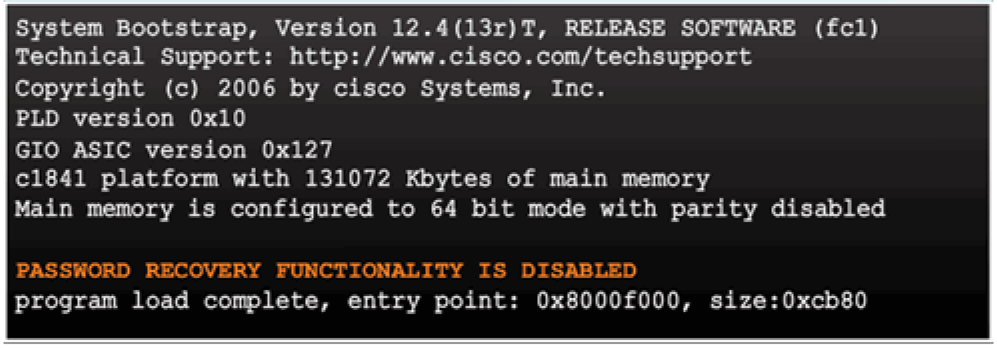
```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery
 mechanism.
Do not execute this command without another plan for
 password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)#
```

No Service Password Recovery



```
R1# show running-config
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
```

Password Recovery Functionality is Disabled



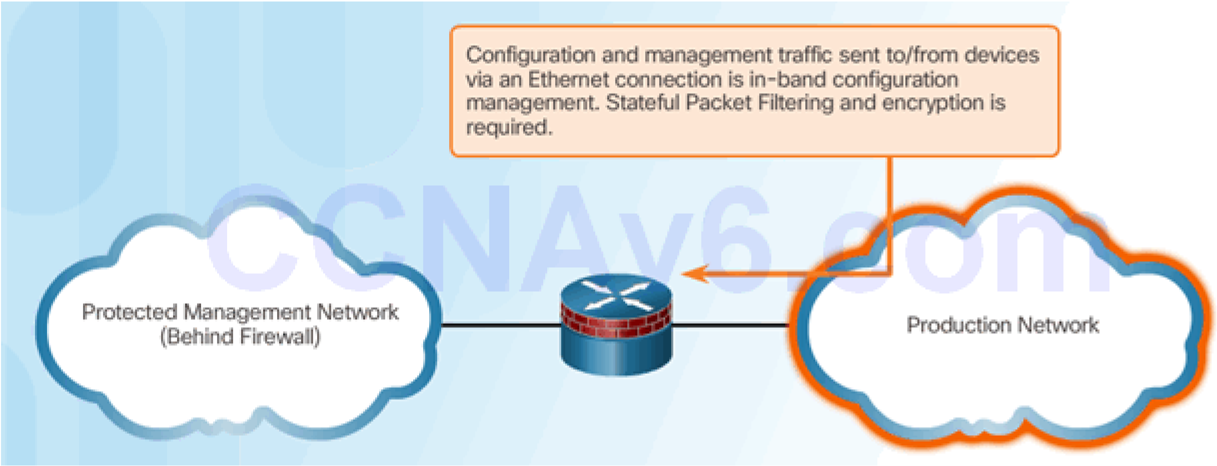
```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity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

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

Topic 2.3.2: Secure Management and Reporting

Determining the Type of Management Access

In-Band Management:

- Apply only to devices that need to be managed or monitored
- Use IPsec, SSH, or SSL when possible
- Decide whether the management channel need to be open at all time

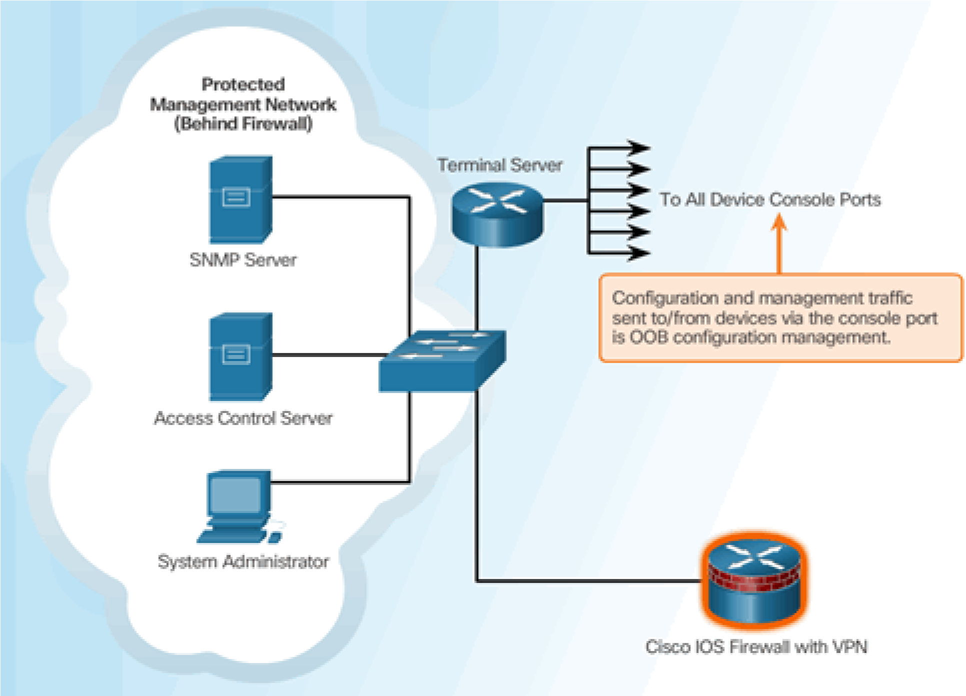


Configuration and management traffic sent to/from devices via an Ethernet connection is in-band configuration management. Stateful Packet Filtering and encryption is required.

Out-of-Band (OOB) Management:

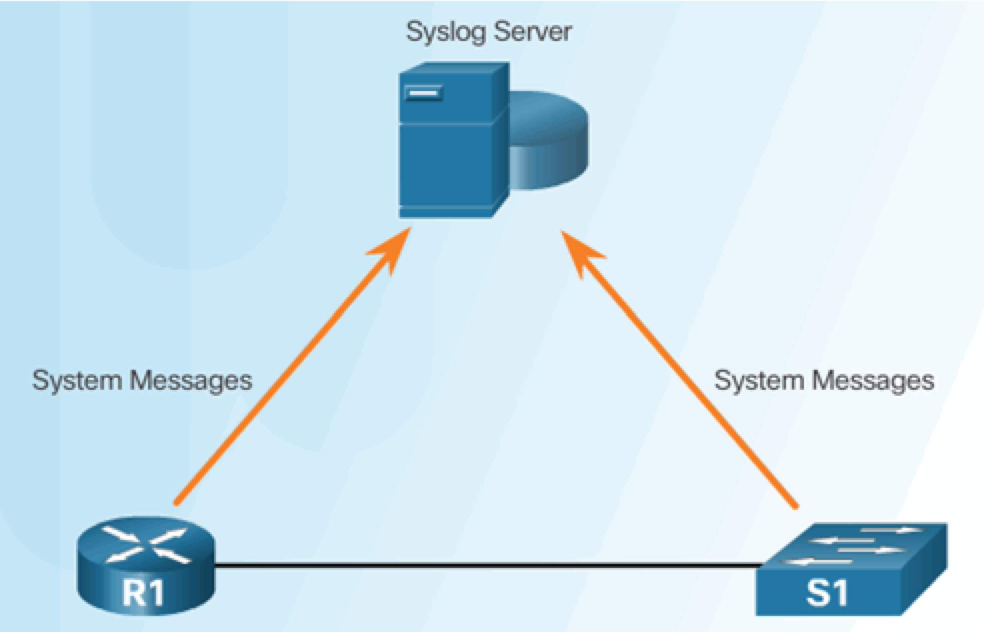
- Provide highest level of security

- Mitigate the risk of passing management protocols over the production network

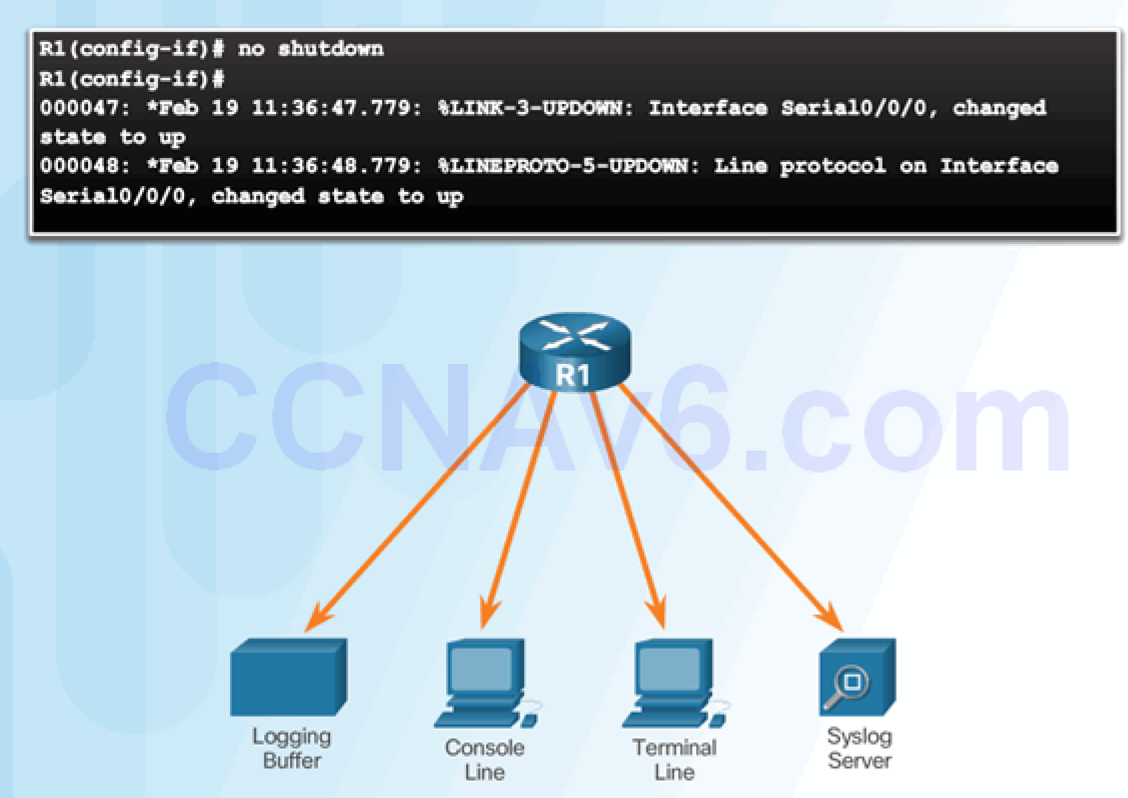

Protected Management Network (Behind Firewall)
SNMP Server
Access Control Server
System Administrator
Terminal Server
To All Device Console Ports
Configuration and management traffic sent to/from devices via the console port is OOB configuration management.
Cisco IOS Firewall with VPN

Topic 2.3.3: Using Syslog for Network Security

Introduction to Syslog



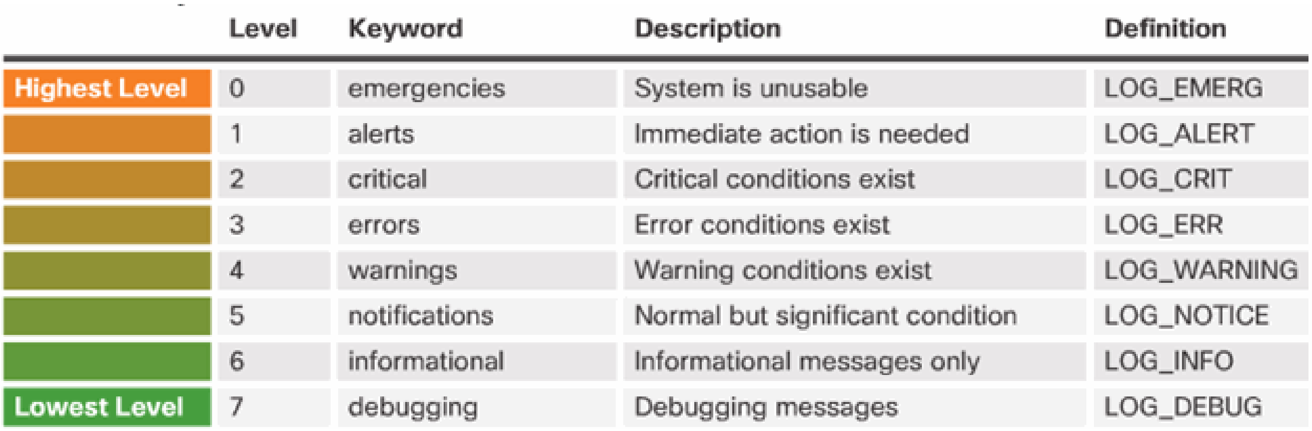
Syslog Operation



```
R1(config-if)# no shutdown
R1(config-if)#
000047: *Feb 19 11:36:47.779: %LINK-3-UPDOWN: Interface Serial0/0/0, changed
state to up
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
```

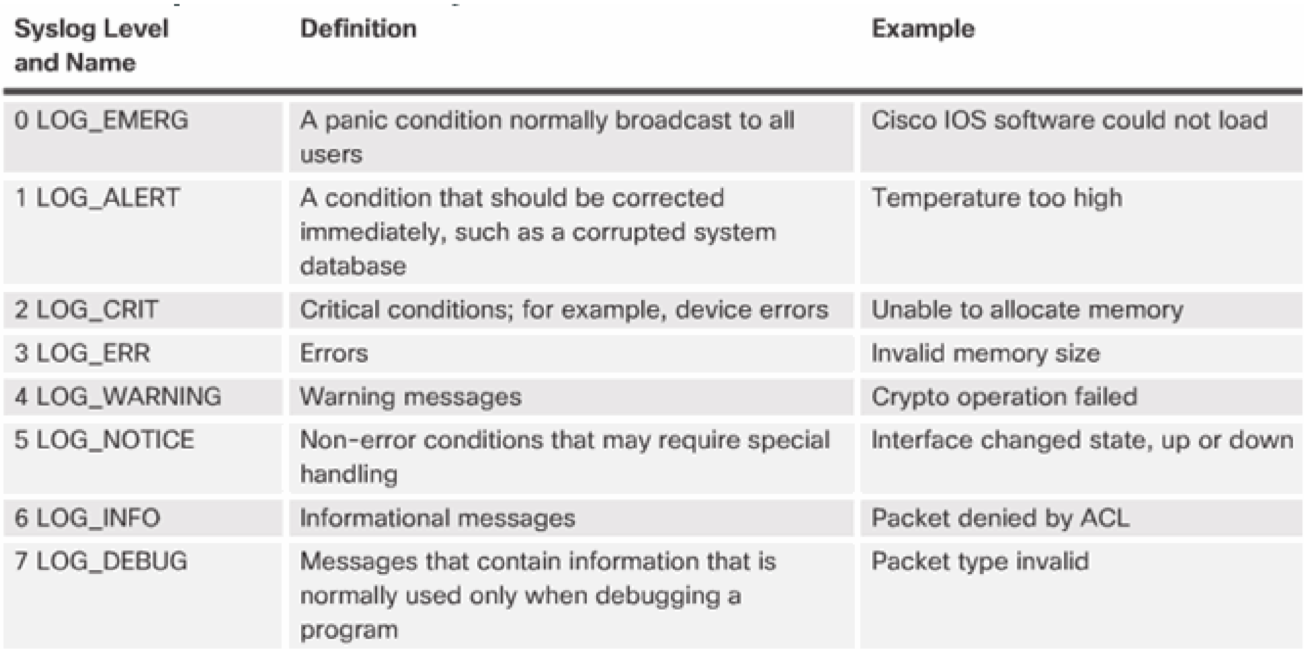
Syslog Message

Security Levels

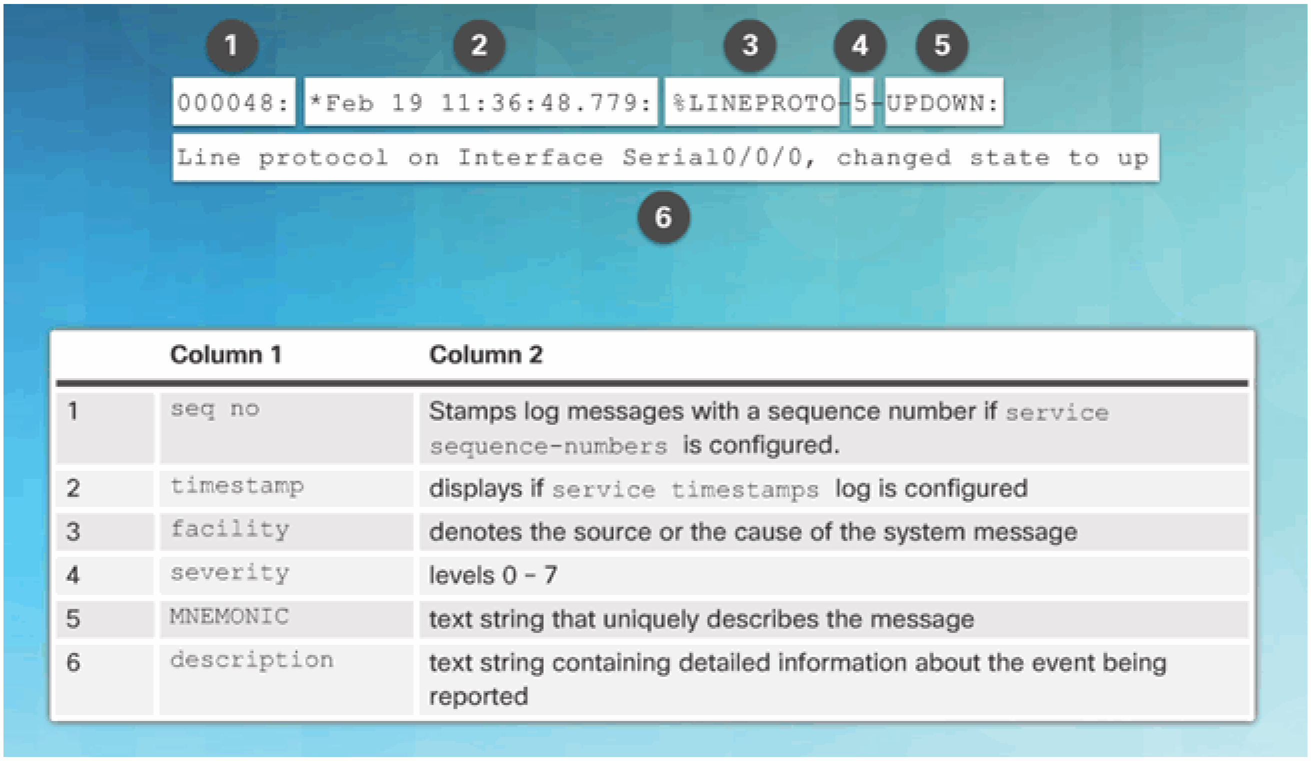


	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal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

Example Severity Levels



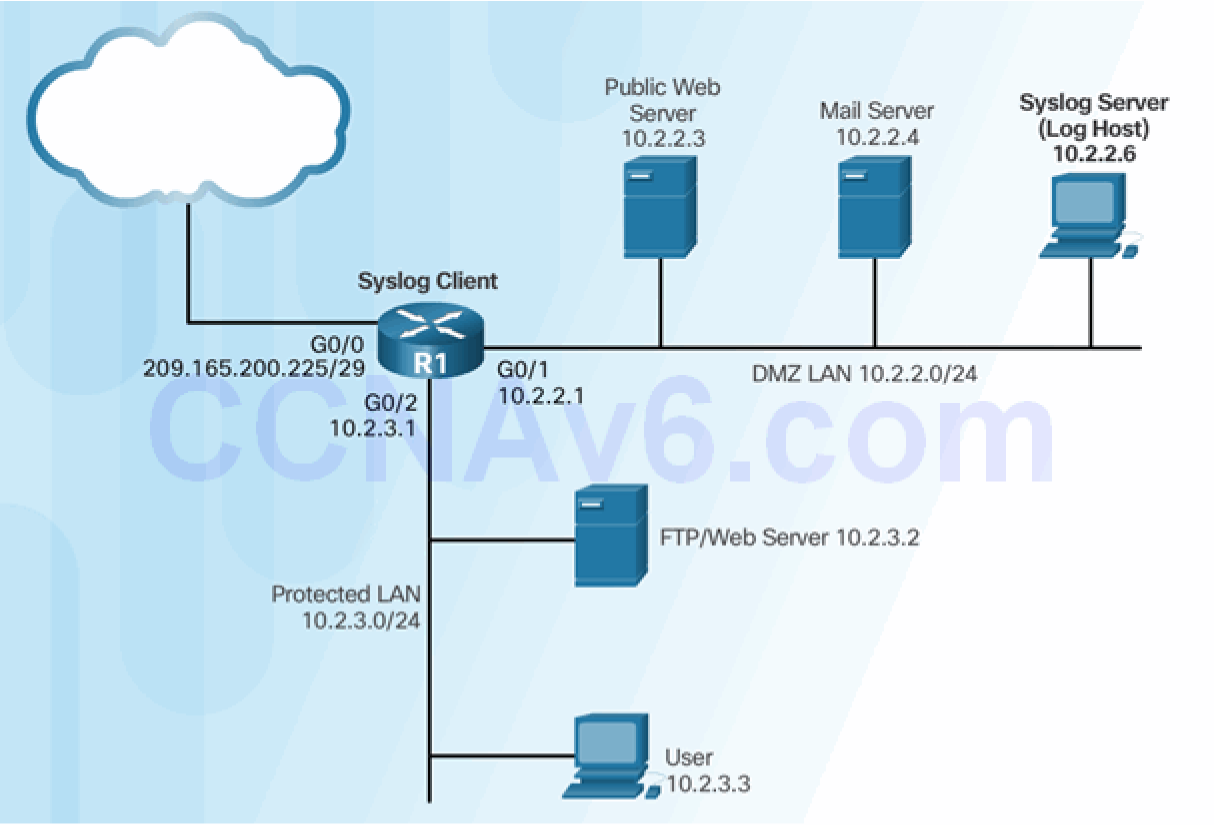
Syslog Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Non-error conditions that may require special handling	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 a program	Packet type invalid



```
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Serial0/0/0, changed state to up
```

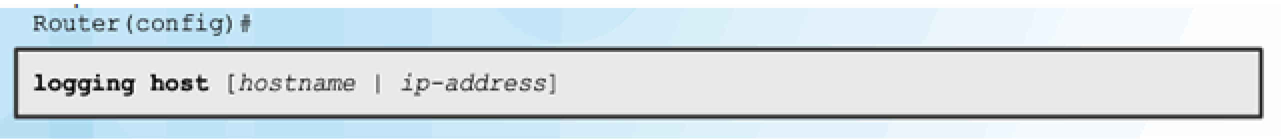
	Column 1	Column 2
1	`seq no`	Stamps log messages with a sequence number if `service sequence-numbers` is configured.
2	`timestamp`	displays if `service timestamps` log is configured
3	`facility`	denotes the source or the cause of the system message
4	`severity`	levels 0 - 7
5	`MNEMONIC`	text string that uniquely describes the message
6	`description`	text string containing detailed information about the event being reported

Syslog Systems



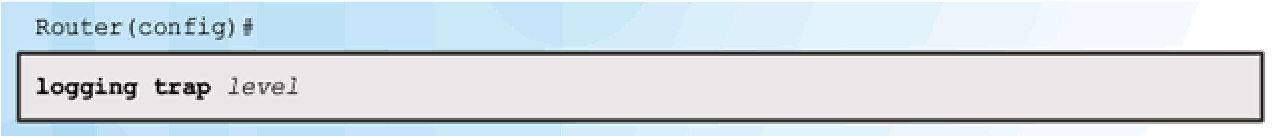
Configuring System Logging

Step 1



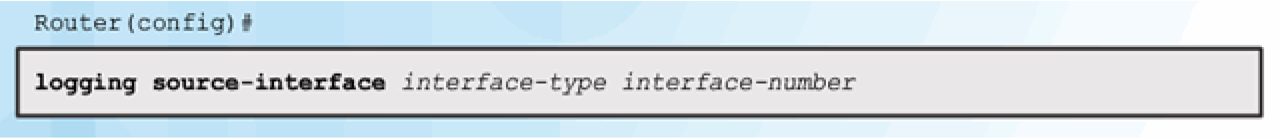
```
Router(config)#
logging host [hostname | ip-address]
```

Step 2 (optional)



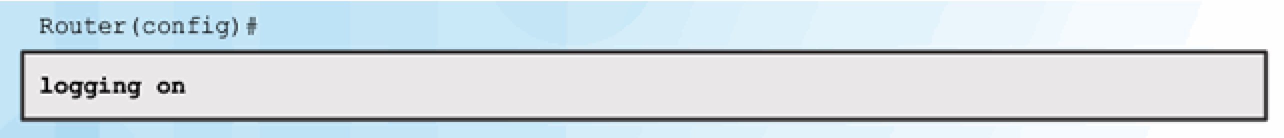
```
Router(config)#
logging trap level
```

Step 3



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

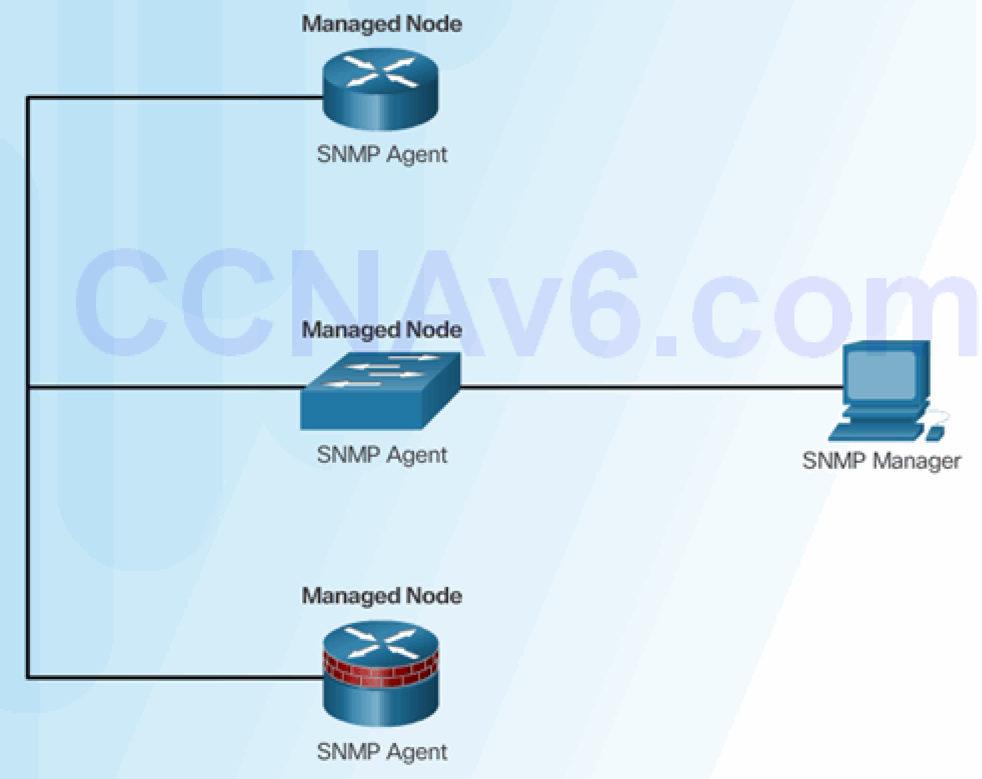
Step 4



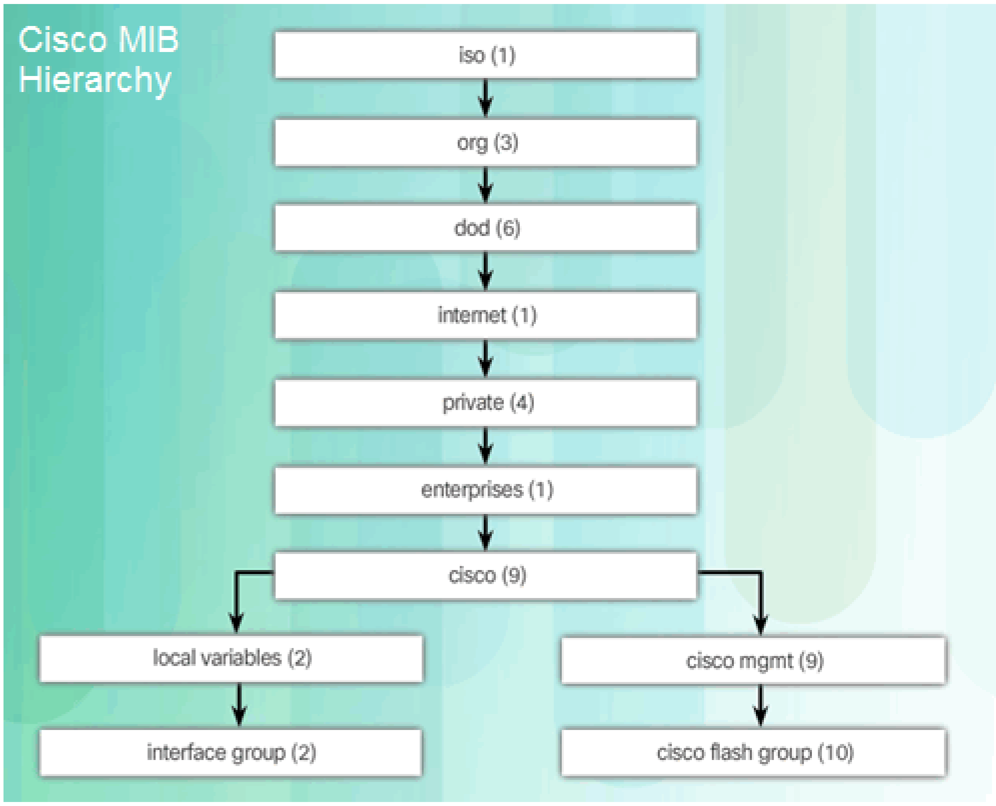
```
Router(config)#
logging on
```

Topic 2.3.4: Using SNMP for Network Security

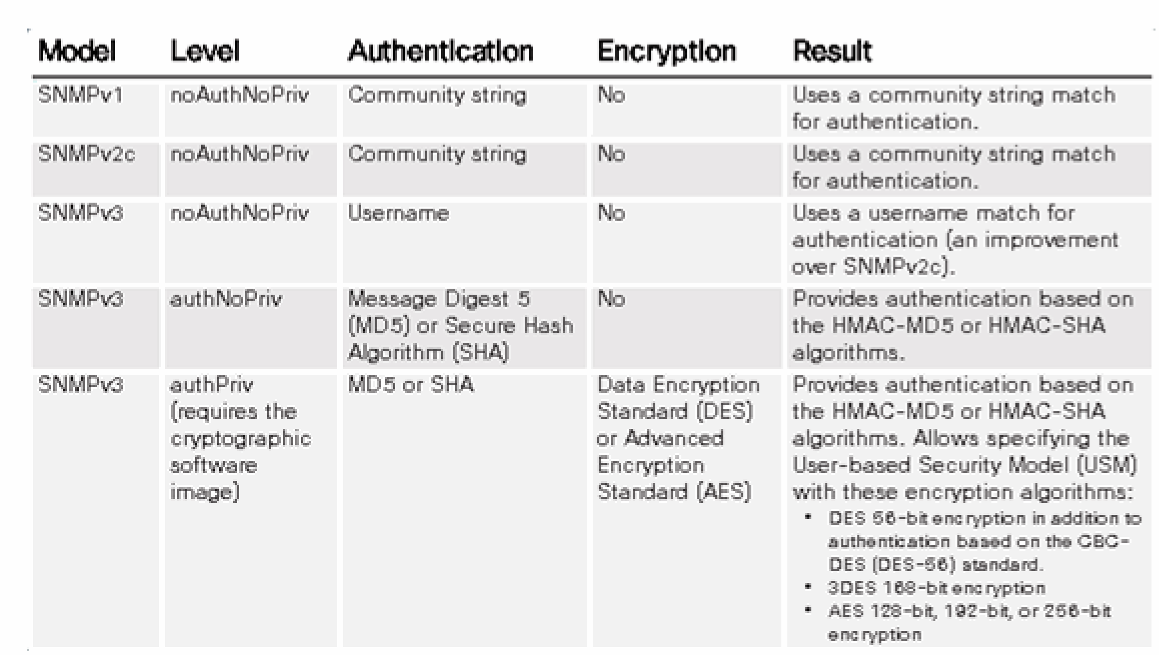
Introduction to SNMP



Management Information Base

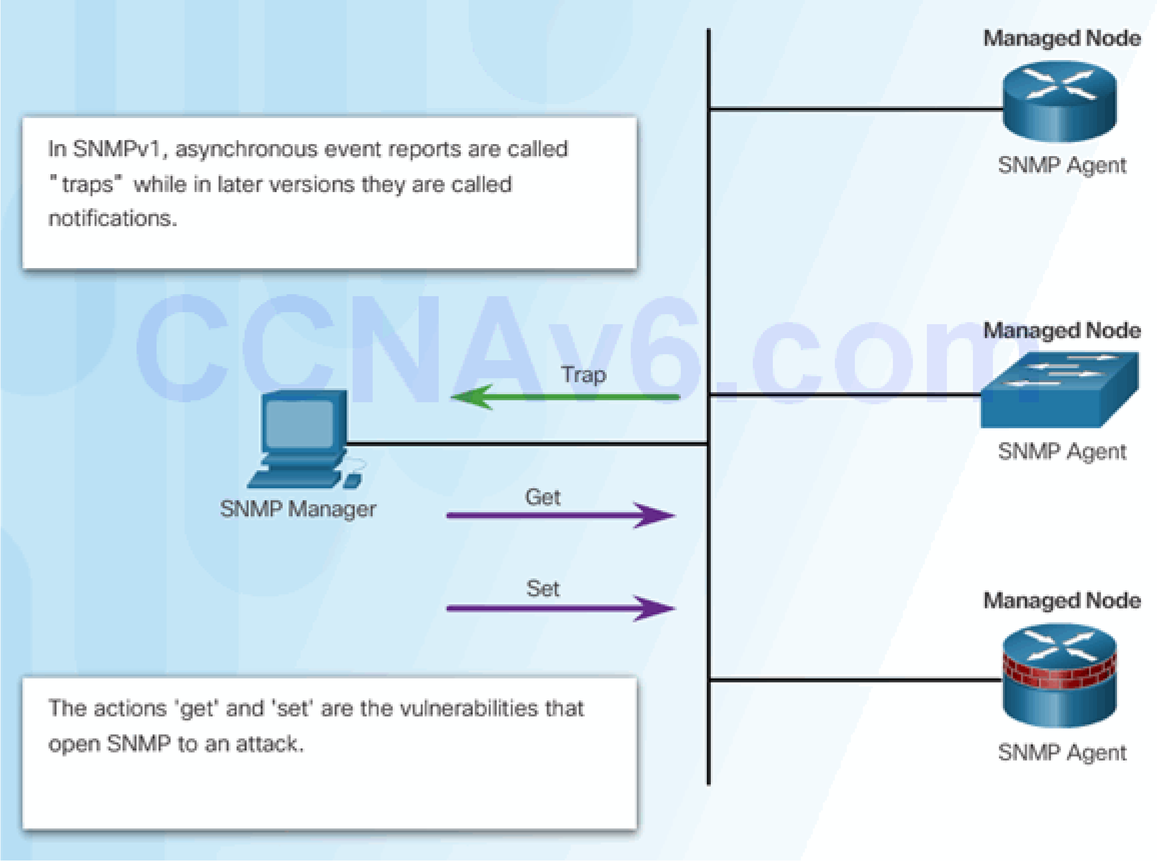


SNMP Versions



Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit encryption • AES 128-bit, 192-bit, or 256-bit encryption

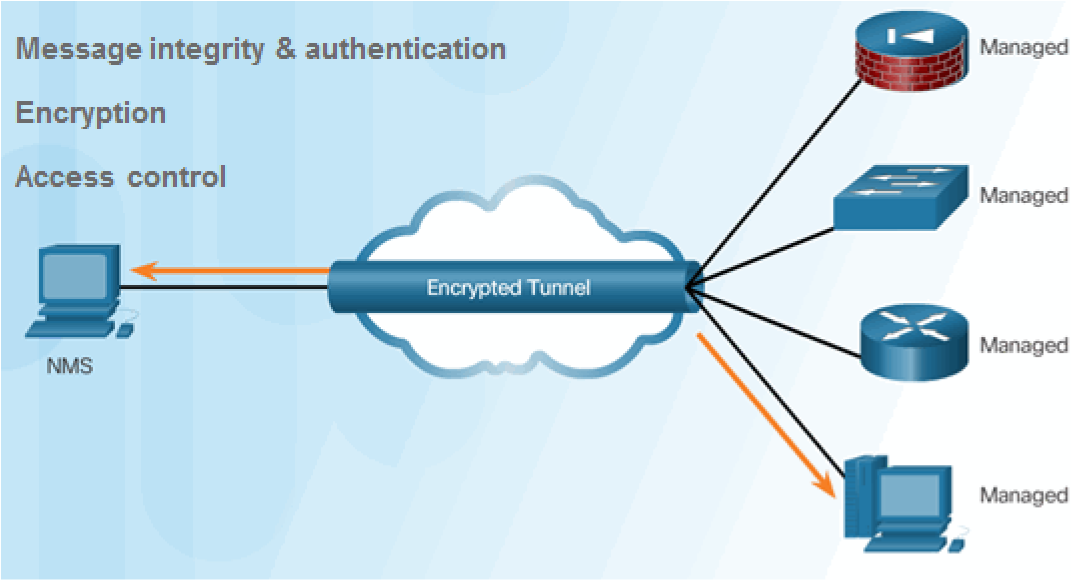
SNMP Vulnerabilities



In SNMPv1, asynchronous event reports are called "traps" while in later versions they are called notifications.

The actions 'get' and 'set' are the vulnerabilities that open SNMP to an attack.

SNMPv3

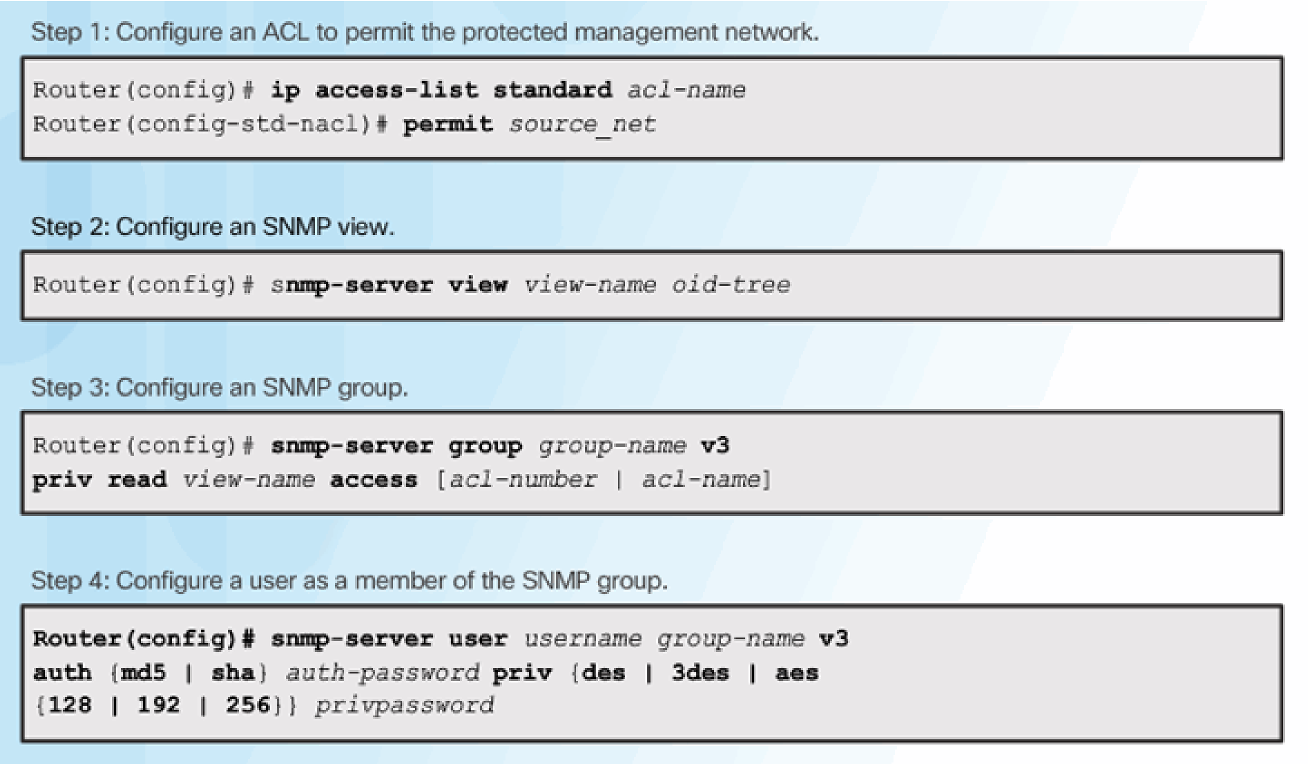

Message integrity & authentication

Encryption

Access control

- Transmissions from manager to agent may be authenticated to guarantee the identity of the sender and the integrity and timeliness of a message.
- SNMPv3 messages may be encrypted to ensure privacy.
- Agent may enforce access control to restrict each principal to certain actions on specific portions of data.

Configuring SNMPv3 Security



Step 1: Configure an ACL to permit the protected management network.

```
Router(config)# ip access-list standard acl-name
Router(config-std-nacl)# permit source_net
```

Step 2: Configure an SNMP view.

```
Router(config)# snmp-server view view-name oid-tree
```

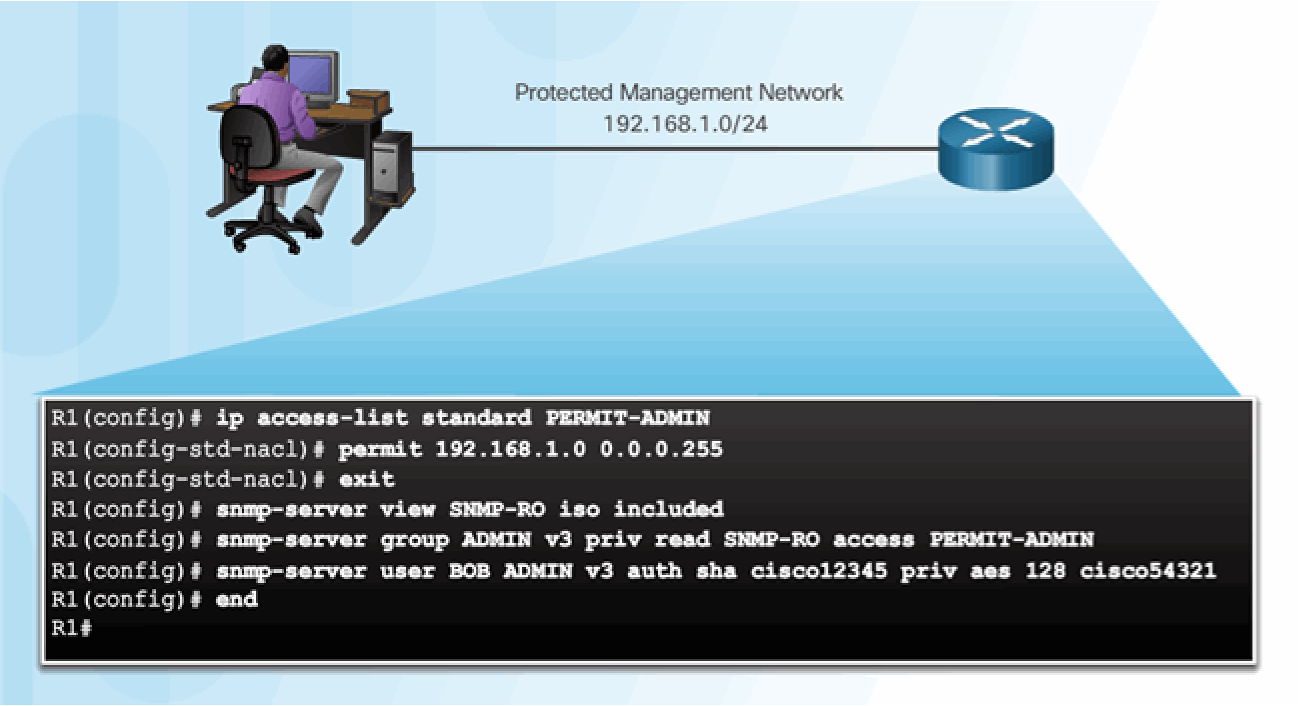
Step 3: Configure an SNMP group.

```
Router(config)# snmp-server group group-name v3
priv read view-name access [acl-number | acl-name]
```

Step 4: Configure a user as a member of the SNMP group.

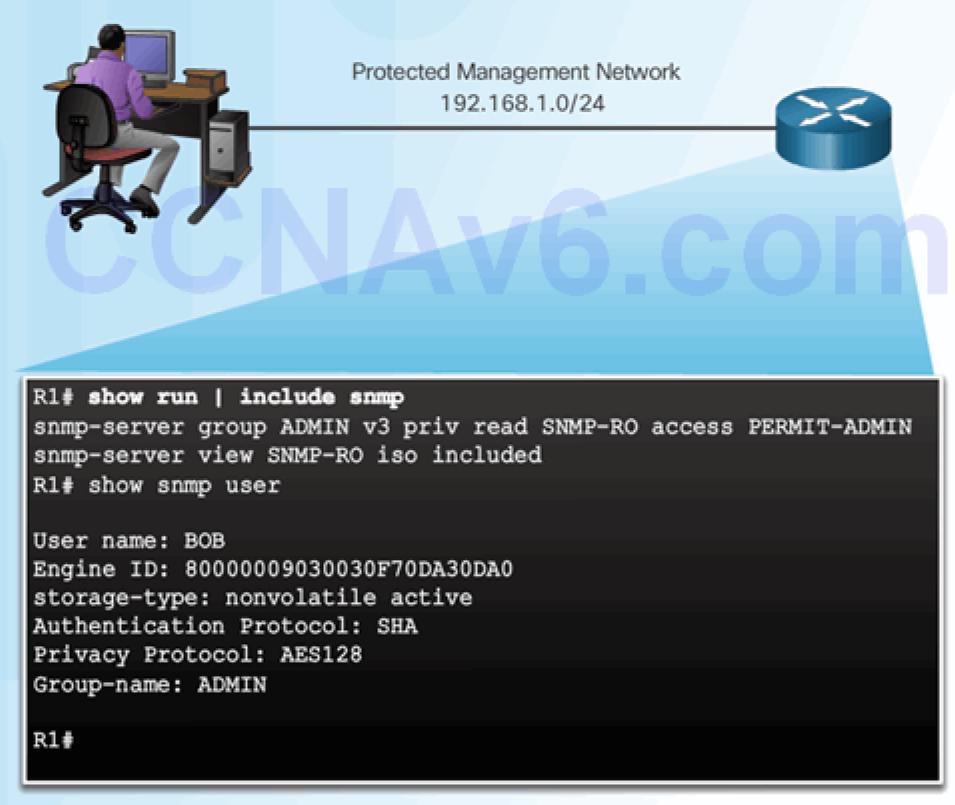
```
Router(config)# snmp-server user username group-name v3
auth {md5 | sha} auth-password priv {des | 3des | aes
{128 | 192 | 256}} privpassword
```

Secure SNMPv3 Configuration Example



```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321
R1(config)# end
R1#
```

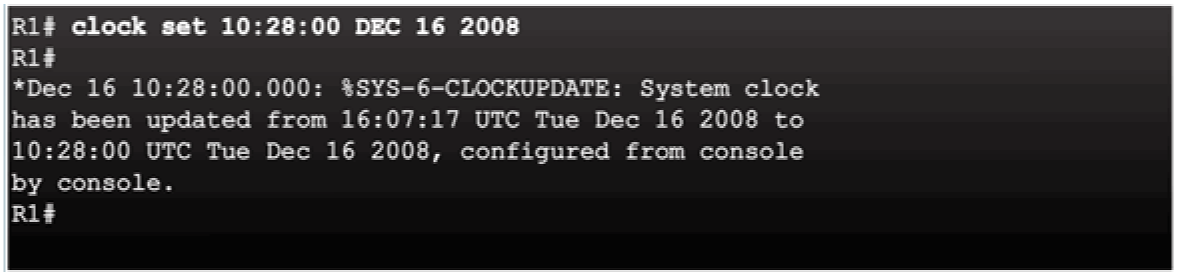
Verifying the SNMPv3 Configuration



```
R1# show run | include snmp
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
snmp-server view SNMP-RO iso included
R1# show snmp user

User name: BOB
Engine ID: 80000009030030F70DA30DA0
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ADMIN

R1#
```

Topic 2.3.5: Using NTP

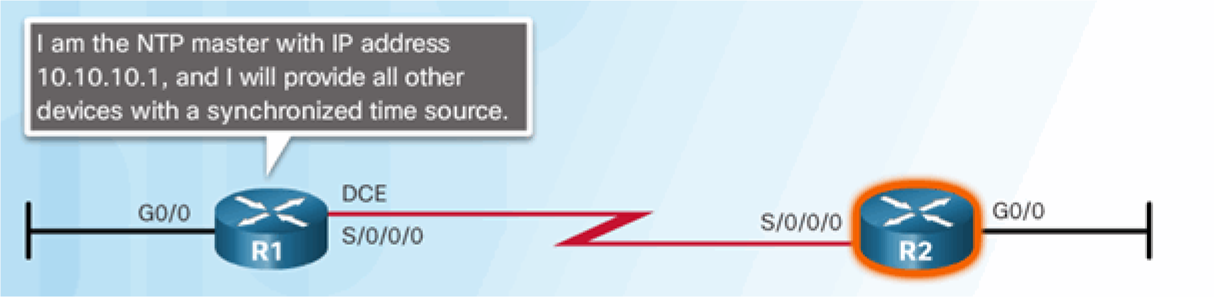
Network Time Protocol



```
R1# clock set 10:28:00 DEC 16 2008
R1#
*Dec 16 10:28:00.000: %SYS-6-CLOCKUPDATE: System clock
has been updated from 16:07:17 UTC Tue Dec 16 2008 to
10:28:00 UTC Tue Dec 16 2008, configured from console
by console.
R1#
```

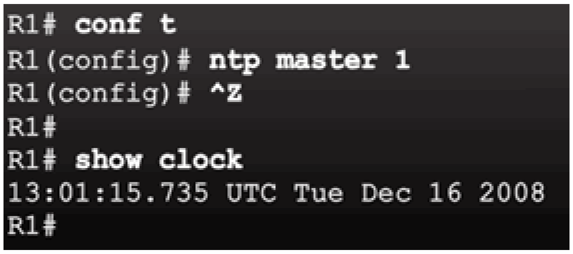
NTP Server

Sample NTP Topology

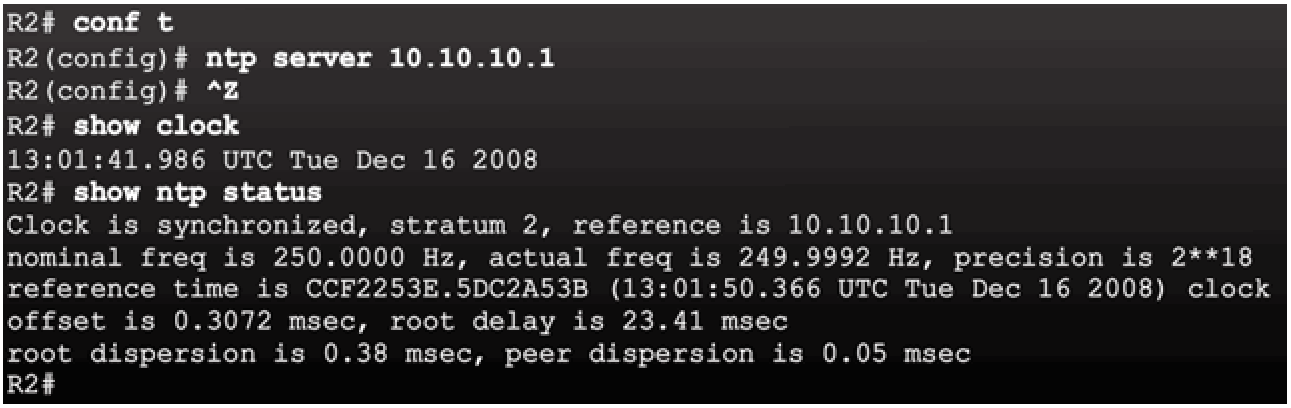

I am the NTP master with IP address 10.10.10.1, and I will provide all other devices with a synchronized time source.
G0/0
R1
DCE
S/0/0/0
S/0/0/0
R2
G0/0

Sample NTP Configuration on R1

Sample NTP Configuration on R2

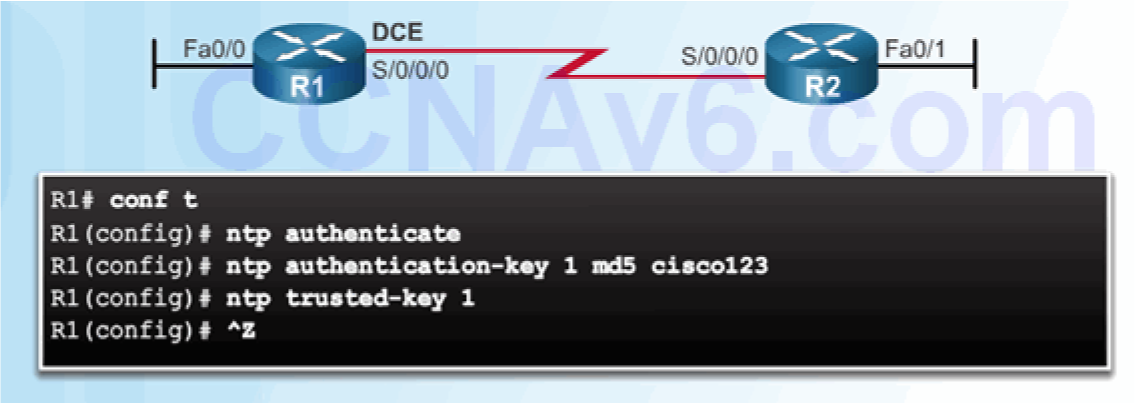


```
R1# conf t
R1(config)# ntp master 1
R1(config)# ^Z
R1#
R1# show clock
13:01:15.735 UTC Tue Dec 16 2008
R1#
```



```
R2# conf t
R2(config)# ntp server 10.10.10.1
R2(config)# ^Z
R2# show clock
13:01:41.986 UTC Tue Dec 16 2008
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.10.10.1
nominal freq is 250.0000 Hz, actual freq is 249.9992 Hz, precision is 2**18
reference time is CCF2253E.5DC2A53B (13:01:50.366 UTC Tue Dec 16 2008) clock
offset is 0.3072 msec, root delay is 23.41 msec
root dispersion is 0.38 msec, peer dispersion is 0.05 msec
R2#
```

NTP Authentication

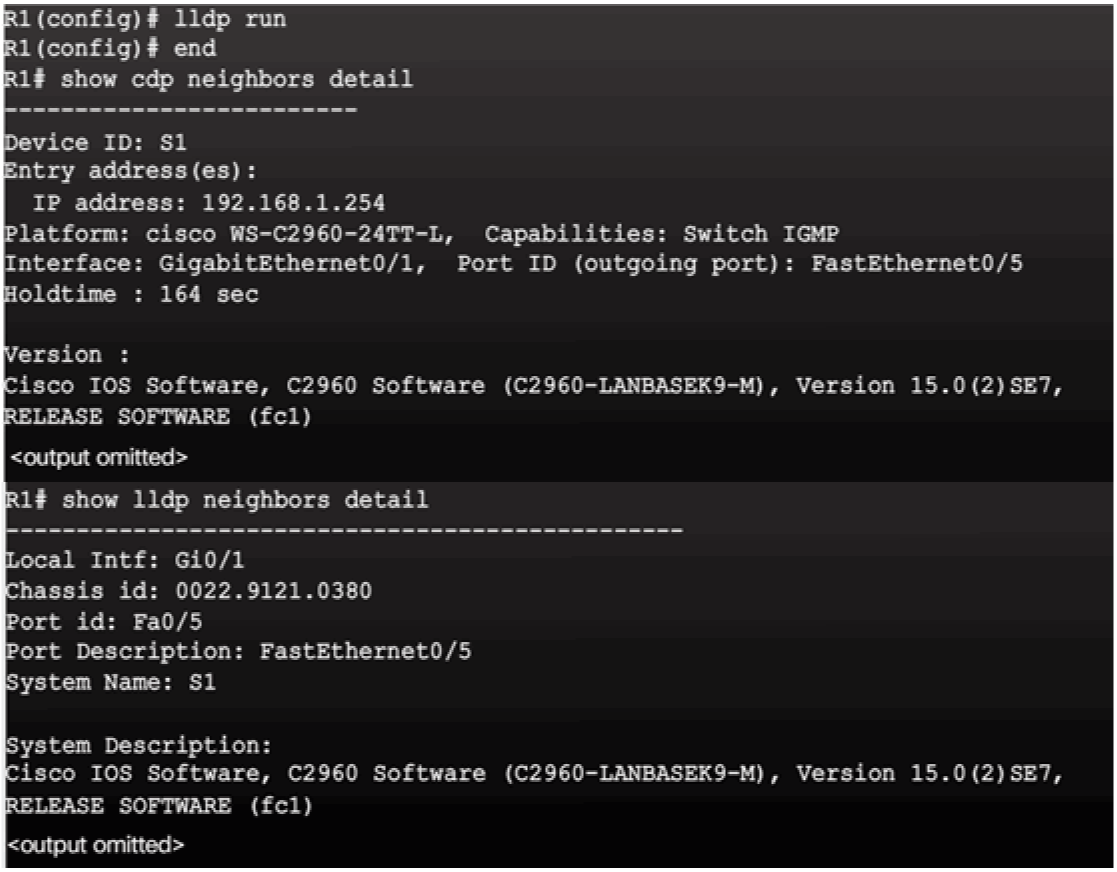


```
R1# conf t
R1(config)# ntp authenticate
R1(config)# ntp authentication-key 1 md5 cisco123
R1(config)# ntp trusted-key 1
R1(config)# ^Z
```

Section 2.4: Using Automated Security Features

Topic 2.4.1: Performing a Security Audit

Discovery Protocols CDP and LLDP



```
R1(config)# lldp run
R1(config)# end
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.254
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 164 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
R1# show lldp neighbors detail
------------------------------------------------
Local Intf: Gi0/1
Chassis id: 0022.9121.0380
Port id: Fa0/5
Port Description: FastEthernet0/5
System Name: S1

System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
```

Settings for Protocols and Services

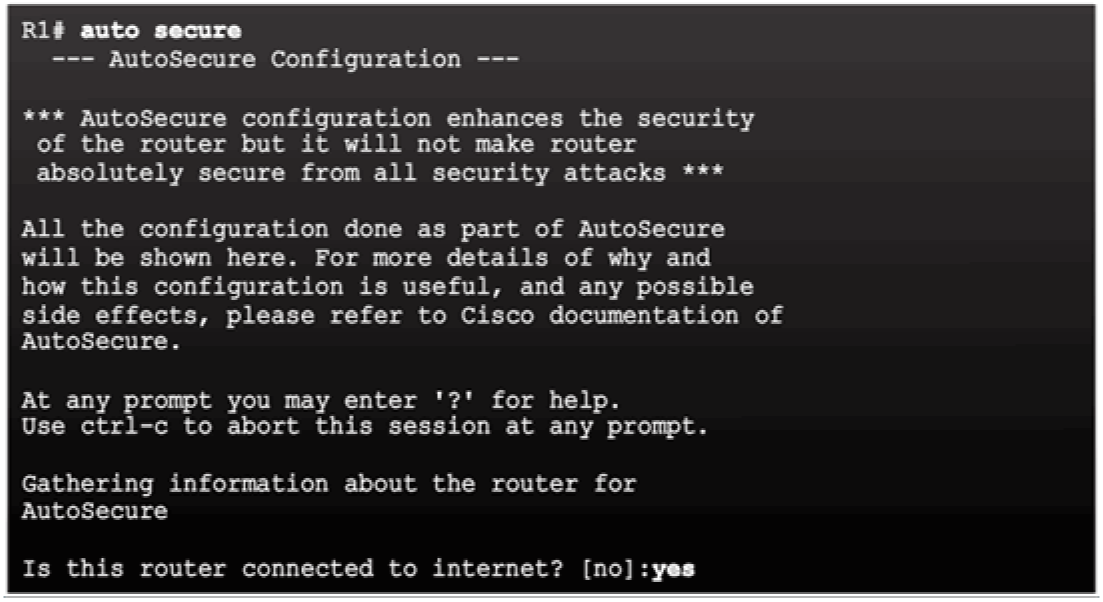
There is a detailed list of security settings for protocols and services provided in Figure 2 of this page in the course.

Additional recommended practices to ensure a device is secure:

- Disable unnecessary services and interfaces.
- Disable and restrict commonly configured management services.
- Disable probes and scans. Ensure terminal access security.
- Disable gratuitous and proxy ARPs
- Disable IP-directed broadcasts.

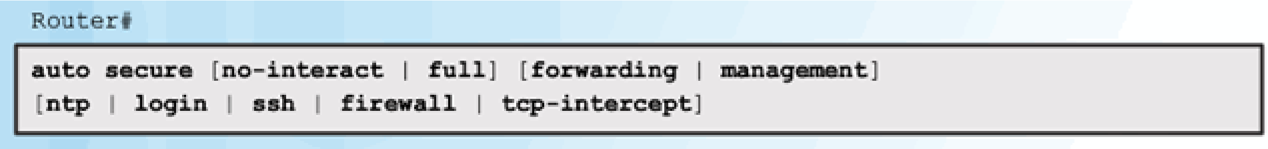
Topic 2.4.2: Locking Down a Router Using AutoSecure

Cisco AutoSecure

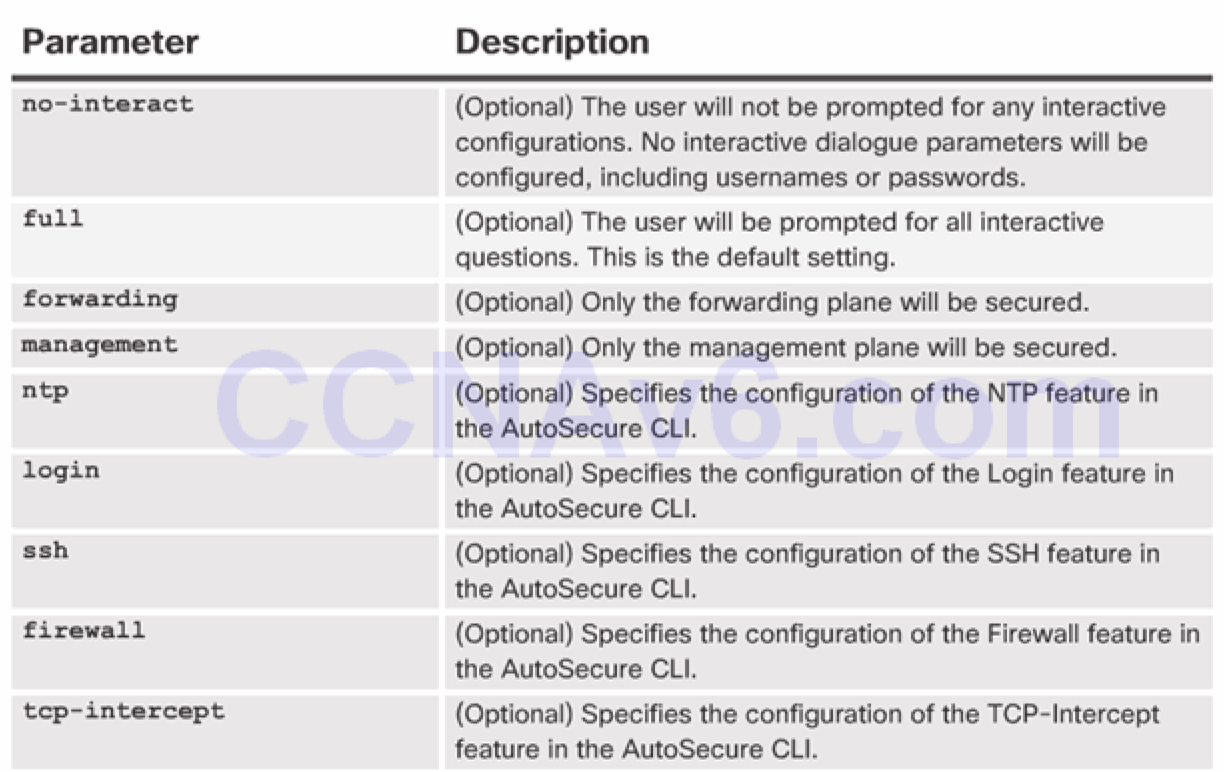


```
R1# auto secure
  --- AutoSecure Configuration ---

*** 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
```

Using the Cisco AutoSecure Feature



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



Parameter	Description
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.
forwarding	(Optional) Only the forwarding plane will be secured.
management	(Optional) Only the management plane will be secured.
ntp	(Optional) Specifies the configuration of the NTP feature in the AutoSecure 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.

Using the auto secure Command

1. The auto secure command is entered

2. Wizard gathers information about the outside interfaces
3. AutoSecure secures the management plane by disabling unnecessary services
4. AutoSecure prompts for a banner
5. AutoSecure prompts for passwords and enables password and login features
6. Interfaces are secured
7. Forwarding plane is secured

Section 2.5: Securing the Control Plane

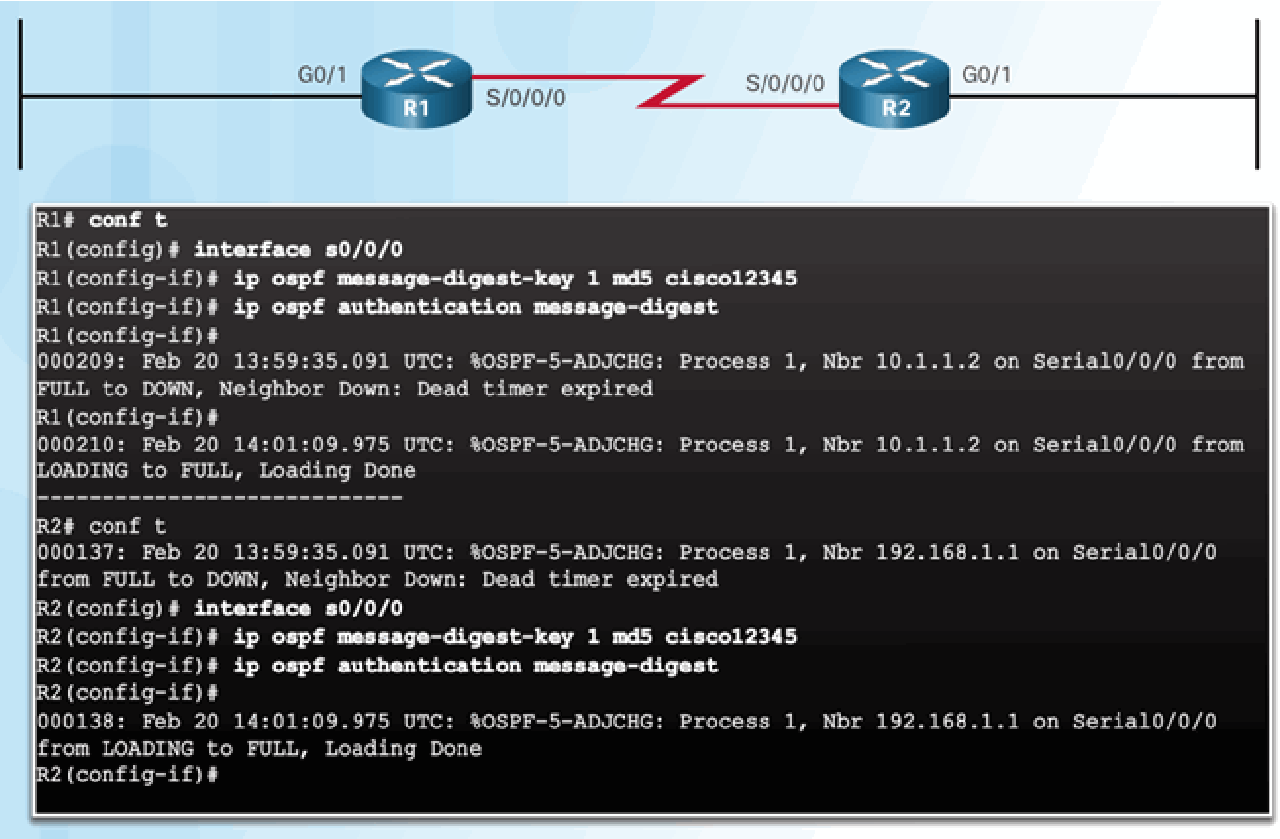
Topic 2.5.1: Routing Protocol Authentication

Routing Protocol Spoofing

Consequences of protocol spoofing:

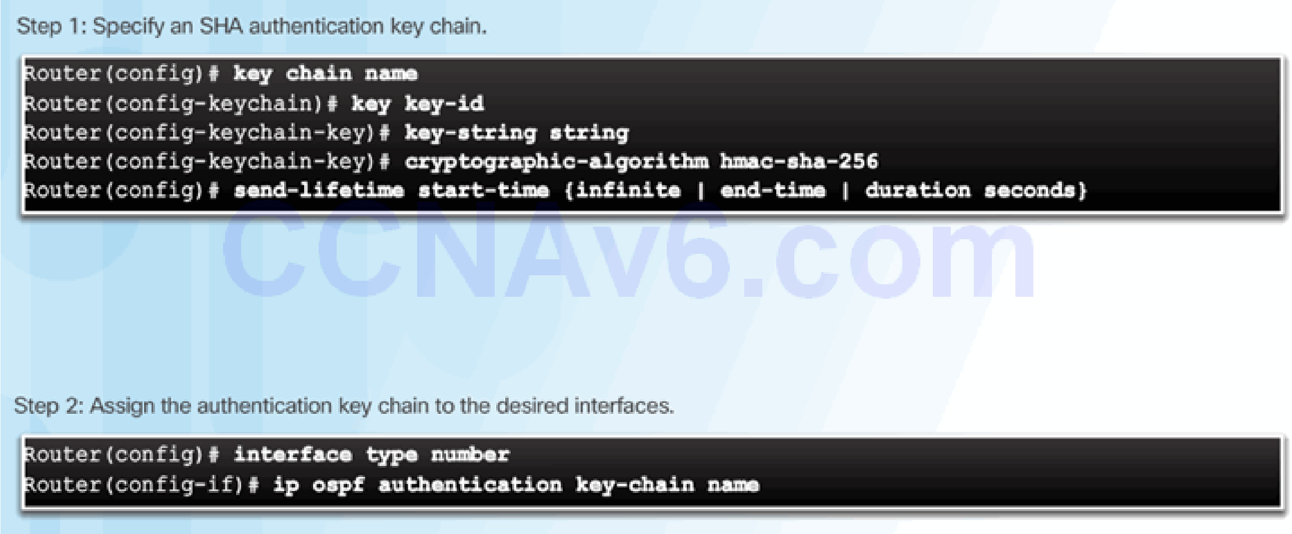
- Redirect traffic to create routing loops.
- Redirect traffic so it can be monitored on an insecure link.
- Redirect traffic to discard it.

OSPF MD5 Routing Protocol Authentication



```
R1# conf t
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R1(config-if)# ip ospf authentication message-digest
R1(config-if)#
000209: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000210: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
LOADING to FULL, Loading Done
----------------------------
R2# conf t
000137: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R2(config)# interface s0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R2(config-if)# ip ospf authentication message-digest
R2(config-if)#
000138: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
R2(config-if)#
```

OSPF SHA Routing Protocol Authentication



Step 1: Specify an SHA authentication key chain.

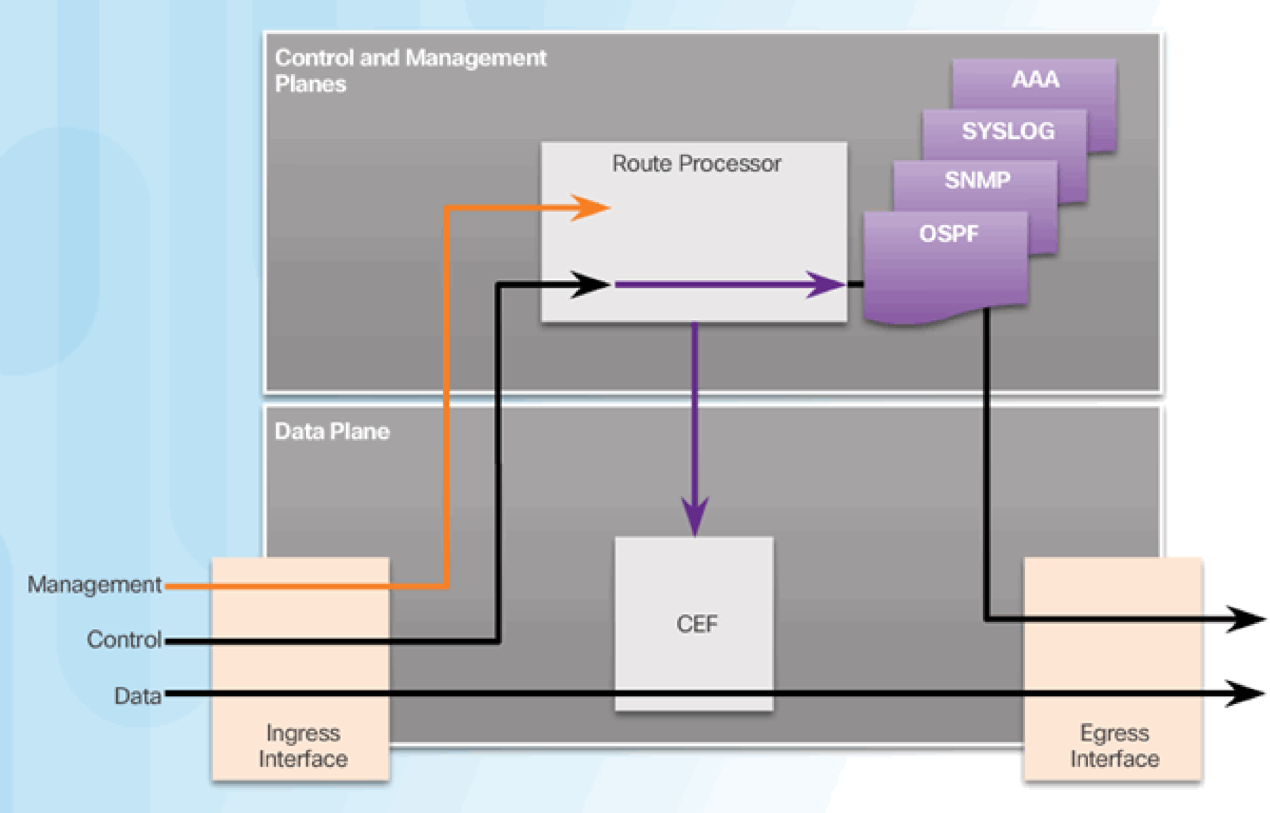
```
Router(config)# key chain name
Router(config-keychain)# key key-id
Router(config-keychain-key)# key-string string
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-256
Router(config)# send-lifetime start-time {infinite | end-time | duration seconds}
```

Step 2: Assign the authentication key chain to the desired interfaces.

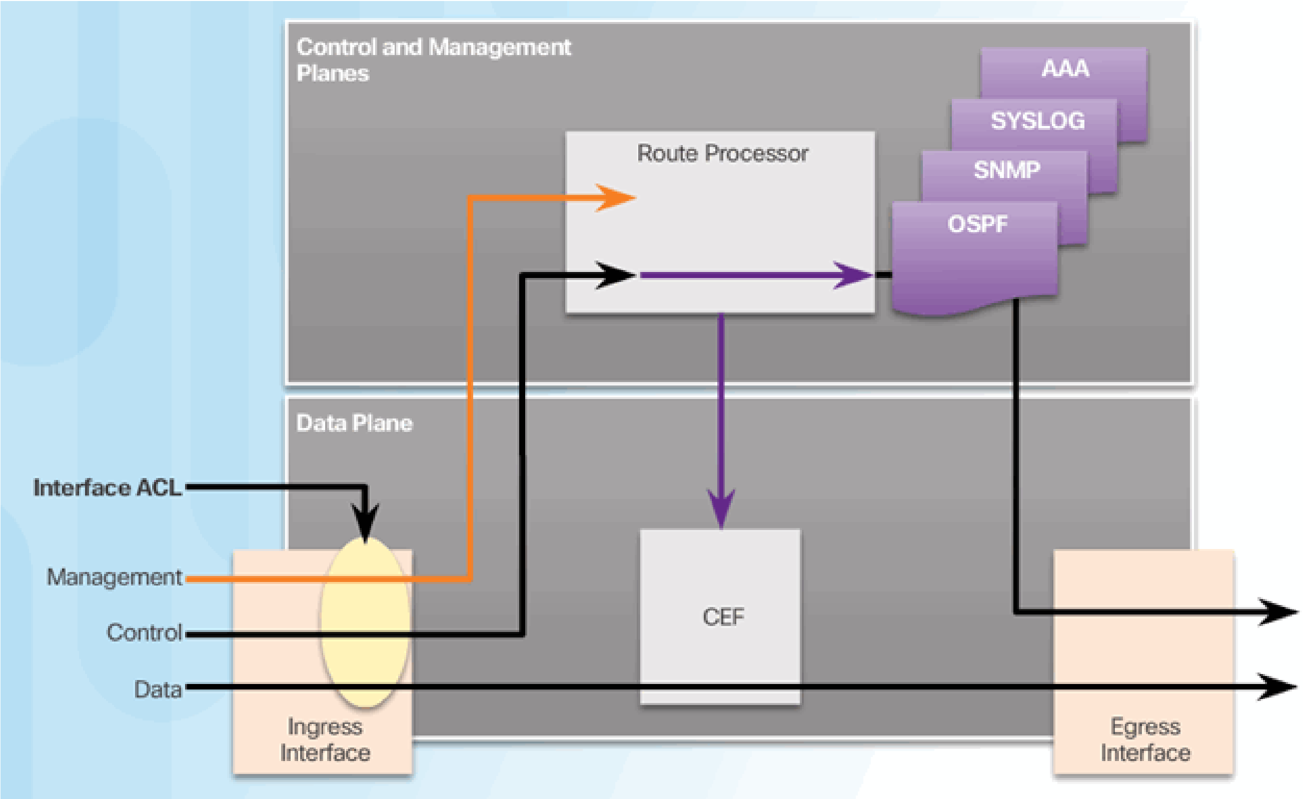
```
Router(config)# interface type number
Router(config-if)# ip ospf authentication key-chain name
```

Topic 2.5.2: Control Plane Policing

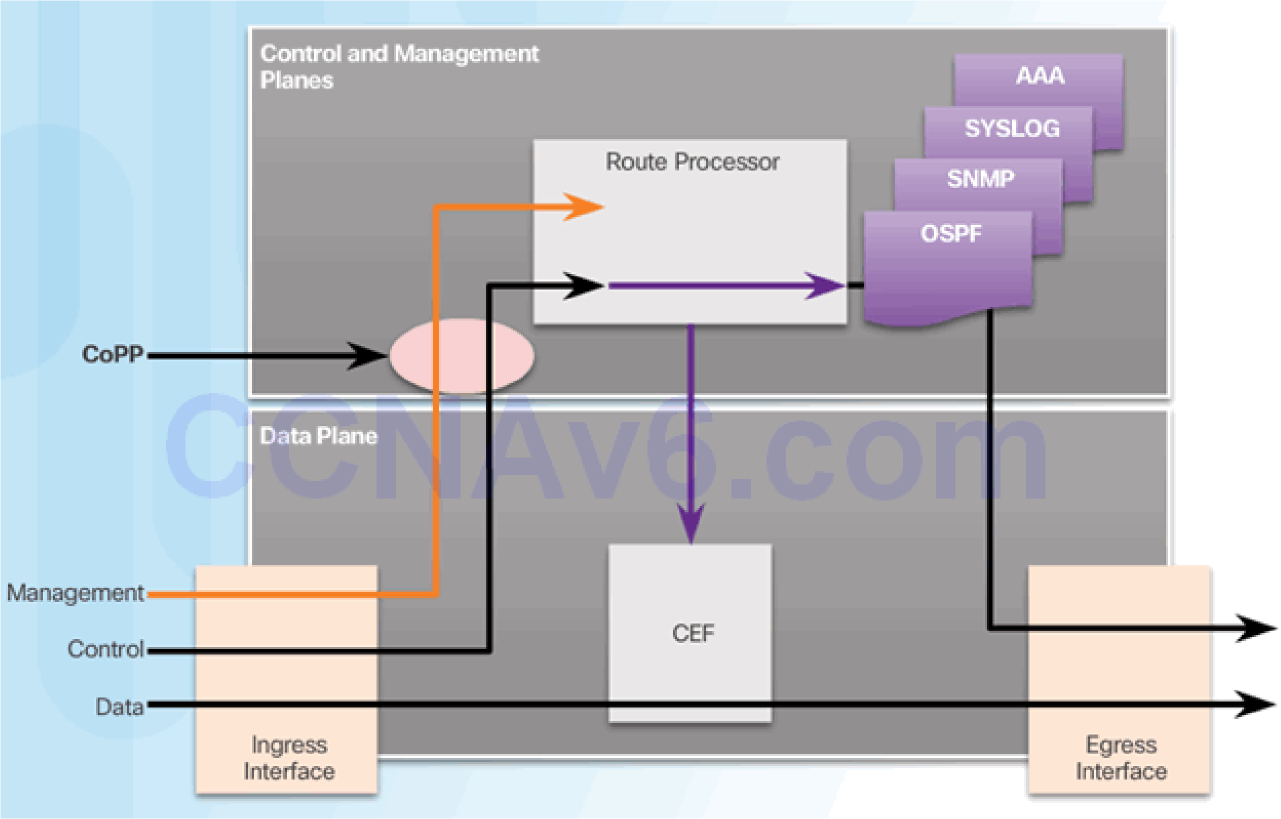
Network Device Operations



Control and Management Plane Vulnerabilities



CoPP Operation



Section 2.6: Summary

Chapter Objectives:

- Configure secure administrative access.
- Configure command authorization using privilege levels and role-based CLI.
- Implement the secure management and monitoring of network devices.
- Use automated features to enable security on IOS-based routers.
- Implement control plane security.

Download Slide PowerPoint (pptx):

[sociallocker id="54558″]

PPT

CCNASv2_InstructorPPT_CH2.pptx **4.64 MB** **2087 downloads**

…

Download

[/sociallocker]